

ENCLOSURE 2

NONDISCLOSURE AGREEMENT FOR CLASSIFIED INFORMATION

1. I, _____ (print full name), hereby agree to accept the obligations contained in this agreement as a prior condition of my being given access to information or material by the United States Government (U.S. Government) that is classified, or is in the process of a classification determination, in accordance with the standards set forth in Executive Order 13526 as amended or superseded, or other applicable Executive order.

2. I understand that such information if disclosed in an unauthorized manner would jeopardize intelligence activities of the U.S. Government. I accept that by being granted access to such information or material I will be placed in a position of special confidence and trust and become obligated to protect that information and/or material from unauthorized disclosure.

3. In consideration for being provided access to information or material by the U.S. Government that is classified, or is in the process of a classification determination in accordance with the standards set forth in Executive Order 13526 as amended or superseded, or other applicable Executive order, I hereby agree that I will never disclose in any form or any manner, to any person not authorized by the U.S. Government to receive it, any information or material in either of the following categories:

- a. information or material, including oral communications, received or obtained pursuant to this agreement with the U.S. Government that is marked as classified or that I have been informed or otherwise know is classified;
- b. information or material, including oral communications, received or obtained pursuant to this agreement with the U.S. Government that I have been informed or otherwise know is in the process of a classification determination.

4. I understand that it is my responsibility to consult with appropriate management authorities in the U.S. Government component that has sponsored my access, or with the prepublication review component of the agency that gave or sponsored my access to classified information if I am no longer associated with the U.S. Government, in order to know: 1) whether information or material within my knowledge or control that I have reason to believe might be in either of the categories set forth in paragraph 3 is considered by the U.S. Government to fit in either of those categories; and, 2) whom the U.S. Government has authorized to receive such information or material.

5. As a further condition of the special confidence and trust reposed in me by the U.S. Government, I hereby agree to submit for review by the U.S. Government, any writing or other preparation in any form, including a work of fiction, which contains any mention of intelligence data or activities, or which contains any other information or material that might be based upon either of the categories set forth in paragraph 3, that I contemplate disclosing publicly or that I have

actually prepared for public disclosure, either during my service with the U.S. Government or at any time thereafter, prior to discussing it with or showing it to anyone who is not authorized to have access to the categories set forth in paragraph 3. I further agree that I will not take any steps toward public disclosure until I have received written permission to do so from the U.S. Government.

6. I understand that the purpose of the review described in paragraph 5 above is to give the U.S. Government an opportunity to determine whether the information or material that I contemplate disclosing publicly contains any information or material that I have agreed not to disclose in accordance with paragraph 3. I further understand that the U.S. Government will act upon my submission and make a response to me within a reasonable time. I further understand that if I dispute the U.S. Government's initial determination on the basis that the information in question derives from public sources, I may be called upon to specifically identify such sources. My failure or refusal to do so may itself result in denial of permission to publish or otherwise disclose the information or material in dispute. I further understand that when otherwise classified information is also available independently in open sources and can be cited by the author the U.S. Government will consider that fact in making its determination on whether the information may be published with the appropriate citations, but I recognize that the U.S. Government retains the right to disallow certain open-source information or citations where, because of the author's U.S. Government affiliation and position the reference might confirm the classified content.

7. I understand that all information or material that I may acquire pursuant to this agreement with the U.S. Government that fits either of the categories set forth in paragraph 3 of this agreement are and will remain the property of the U.S. Government unless or until otherwise determined by an authorized Executive branch official or final ruling of a court of law. I agree that I will not use such information or material for any personal or non-official purposes. I also agree to surrender anything constituting, containing or reflecting such information or material upon the conclusion of my employment or other service with the U.S. Government. I further agree to surrender anything constituting, containing, or reflecting such information or material, upon demand by an appropriate official of the U.S. Government.

8. I agree to notify the U.S. Government immediately in the event that I am called upon by judicial or Congressional authorities, or by specially established investigatory bodies of the Executive branch, to testify about, or provide, information or material that I have agreed herein not to disclose. In any legally authorized communications with any such authority or body, I shall observe all applicable rules or procedures for ensuring that information and/or material that is classified or in the process of a classification determination is handled in a secure manner.

9. I understand that nothing contained in this agreement prohibits me from reporting intelligence activities that I consider to be unlawful or improper directly to the Intelligence Oversight Board established by the President, or to any successor body that the President may establish, or to the Senate Select Committee on Intelligence or the House Permanent Select Committee on Intelligence. I recognize that there are also established procedures for bringing such matters to the attention of Inspector General of the agency that gave or sponsored my access to classified information or to the head of the agency that gave or sponsored my access to classified

information. In making any report referred to in this paragraph, I will observe all applicable rules and procedures for ensuring the secure handling of any information or material that may be involved. I understand that any such information or material continues to be subject to this agreement for all other purposes and that such reporting does not constitute public disclosure or declassification of that information or material.

10. I understand that any breach of this agreement by me may result in the U.S. Government taking administrative action against me, if applicable, which can include suspension or termination of my security clearance and relationship with the U.S. Government. I understand that if I violate the terms of this agreement, the U.S. Government may institute a civil proceeding to seek damages or other appropriate relief. Further, I understand that the disclosure of information that I have agreed herein not to disclose can, in some circumstances, constitute a Federal criminal offense.

11. I understand that the U.S. Government may, prior to any unauthorized disclosure that is threatened by me, choose to apply to any appropriate court for an order enforcing this agreement. Nothing in this agreement constitutes a waiver on the part of the United States to institute a civil or criminal proceeding for any breach of this agreement by me. Nothing in this agreement constitutes a waiver on my part of any possible defenses I may have in connection with either civil or criminal proceedings that may be brought against me.

12. In addition to any other remedy to which the U.S. Government may become entitled, I hereby assign to the U.S. Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any divulgence, publication, or revelation of information or material by me that is carried out in breach of paragraph 5 of this agreement or that involves information or material prohibited from disclosure by the terms of this agreement.

13. I understand and accept that, unless I am provided a written release from this agreement or any portion of it by the head of the agency that gave or sponsored my access to classified information or his or her authorized representative, all the conditions and obligations accepted by me in this agreement apply during my service with the U.S. Government, and at all times thereafter.

14. I understand that the purpose of this agreement is to implement the protection of intelligence sources and methods under the National Security Act of 1947, as amended, and Executive Order 12333, as amended.

15. Nothing in this agreement bars disclosures to Congress or disclosures to an authorized official of an executive agency that are deemed essential to reporting of a violation of United States law.

16. I understand that nothing in this agreement limits or otherwise affects any provision of criminal or other law that may be applicable to the unauthorized disclosure of classified information, including the espionage laws (sections 793, 794 and 798 of title 18, United States Code) and the Intelligence Identities Act of 1982 (P.L. 97-200; 50 U.S.C. §3121 *et. seq.*).

17. Each of the numbered paragraphs and lettered subparagraphs of this agreement is severable. If a court should find any paragraphs or subparagraphs of this agreement to be unenforceable, I understand that all remaining provisions will continue in full force.

18. I make this agreement in good faith, and with no purpose of evasion.

19. This agreement shall be interpreted under and in conformance with the law of the United States.

Signature

Date

Social Security Number (See Notice below)

The execution of this agreement was witnessed by the undersigned, who accepted it on behalf of the U.S. Government as a prior condition of access to classified information by the person whose signature appears above.

WITNESS AND ACCEPTANCE:

Signature

Printed Name

Date

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

Home>About CIA-Publications Review Board

Keeping Secrets Safe: The Publications Review Board

All CIA officers, as a condition of employment, sign the standard CIA secrecy agreement when entering on duty. All contractors sign a secrecy agreement that is consistent with the terms and conditions of their contract. A secrecy agreement doesn't oblige officers and contractors to absolute silence, but it does require them to keep national security secrets for as long as the US Government deems the information to be classified. This is a lifelong obligation. In order to help avoid the damage to national security and to the Agency's mission that disclosing classified information would inflict, the CIA created the Publications Review Board (PRB) to preview materials produced by CIA personnel— former and current (both employees and contractors) – to determine if they contain such classified information before they are shared with publishers, blog-subscribers, a TV audience, ghost-writers, co-authors, editors, family members, assistants, representatives, or anyone else not authorized to receive or review such classified information.

What Must Be Submitted to the PRB?

Current and former CIA officers and contractors who have signed the standard CIA secrecy agreement are required to submit to the PRB any and all materials they intend to share with the public that are intelligence related, such as materials that mention the CIA or intelligence activities, or that concern topics to which they had access to classified information while employed at or performing contractual work for CIA. This submission requirement extends beyond the sub-set of topics they may have had immediate responsibility for on a day-to-day basis.

Publishing: Publishing is more than having a printing house bind copies of a book. It means communicating by any means (including orally or electronically), information regardless of form to any person or entity other than the CIA's PRB or a US Government official authorized by the CIA to receive such information for prepublication review. This encompasses materials including but not limited to: book reviews, Op-ed pieces, scholarly papers, scripts, screenplays, blogs, speeches, and other materials. Thus, material covered by a CIA Secrecy Agreement requiring prepublication review must be submitted and approved prior to discussing the material with or showing it to individuals such as a publisher, co-author, agent, editor, ghost-writer, personal representative, family member, or assistant.

Relating to CIA or intelligence activities: Not everything former and current CIA officers and contractors write requires prepublication review. For example, the prepublication requirement does not apply to material such as gardening, wine tasting, stamp collecting, sports and so forth, because they are outside of the purview of the CIA mission or intelligence. However, commentary on matters such as intelligence operations or tradecraft (even fictional works),

foreign intelligence, foreign events of intelligence interest, one's career, scientific or technological developments discussed in an intelligence context, and other topics that touch upon CIA interests or responsibilities need PRB approval.

Why Do Materials Need To Be Reviewed?

In addition to protecting national security, the PRB is also protecting CIA officers and contractors from legal liability. For instance, one may unwittingly share insights on events and capabilities that are thought to be public knowledge, but in fact have not been officially released by the CIA or the US Government. Accidental disclosure is still disclosure, and opens a person up to possible civil or criminal penalties. The PRB helps current and former CIA officers and contractors avoid this by identifying problematic material and working with them to find ways to make their points, while avoiding classified information disclosure. For instance, PRB staff often compare declassified material found at the CIA's [FOIA Reading Room](#) and [CIA.gov](#) with materials submitted for review.

What Kind of Information Might Be Classified?

As outlined in [Executive Order 13526](#) (sec. 1.4), the following categories of information may be classified if unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security:

- military plans, weapons systems, or operations;
- foreign government information;
- intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- foreign relations or foreign activities of the United States, including confidential sources;
- scientific, technological, or economic matters relating to the national security;
- United States Government programs for safeguarding nuclear materials or facilities;
- vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
- the development, production, or use of weapons of mass destruction.

In combination with these criteria, authors are encouraged to ask the following questions during the writing process to get an idea of what information the PRB is protecting:

“As worded, does the text reveal classified information? Why is this information classified [or not]?”

“Would releasing this information damage national security or harm CIA’s intelligence sources and methods?”

Some individual pieces of information may not cause national security damage when standing alone, but can do so if compiled with other information. Also, the PRB is not authorized to release official records or text from Government documents. Individuals seeking such information may submit a FOIA or Privacy Act Request using the procedures found [here](#) and [here](#), respectively.

Resume Prepublication Review

One of the challenges of a career in intelligence is composing a resume that doesn’t reveal any secrets. Although many details of the Agency’s work are classified, a lot of information about [CIA jobs](#) are publicly available. These occupational descriptions are great examples of what current and former Agency officers can share about their work, and provide a good basis on which to prepare resumes and memoirs that will smoothly pass through the prepublication review process. In addition, the guidelines below may be generally helpful for avoiding content that is problematic for prepublication review. Remember – some things CANNOT be used:

- **Countries** – Use regional terms instead of specific cities or countries.
- **Agency-specific** - Use general training or software descriptions as opposed to the specific names or titles, which may be classified.
- **Names** - Do not use names of people and/or places. Please contact the Publications Review Board before using Agency colleagues as references.
- **Numbers** – Use general terms to describe budget information and/or personnel information (e.g., “hundreds” or “millions” or “several”)
- **Office** - Do not use organizational names below the office level (e.g., avoid group or branch names).
- **Technical details** - Use general terms instead of the specific details.

How To Reach Us?

The PRB exists to help protect against unauthorized disclosures, but ultimately, each CIA officer or contractor is responsible for protecting any classified information they possess. Should a CIA officer or contractor publish materials that contain classified information – either because they did not comply with the PRB’s changes or because they chose to bypass the PRB process by not submitting their manuscript for PRB pre-publication review – they could be subject to possible civil and criminal penalties. Cooperating with pre-publication review helps keep CIA officers, contractors, and the Agency safe.

Former Agency officers and contractors who need to contact the PRB regarding items to be reviewed can do so through the [Contact CIA](#) page. (If using the web form, please be sure to fill out the form completely, including your full legal name and email address where you can be reached).

Posted: Jan 07, 2016 12:40 PM

Last Updated: Feb 02, 2017 11:49 AM

UNCLASSIFIED//~~FOUO~~

(U) Disseminating or sharing any part of this document outside CIA must comply with AR 10-16.

AR 13-10 (U//~~FOUO~~) AGENCY PREPUBLICATION REVIEW OF CERTAIN MATERIAL PREPARED FOR PUBLIC DISSEMINATION (Formerly AR 6-2)

AGENCY REGULATION SERIES 13 (SPECIAL REPORTING REQUIREMENTS/RESTRICTIONS), PUBLISHED ON 25 JUNE 2011

Regulation Summary

Ingested from Regulations.cia on 10 May 2013

Policy

REVISION SUMMARY: 25 June 2011

This regulation supersedes AR 6-2, dated 19 July 2010.

AR 6-2 is revised to clarify the prepublication review criteria applicable to the submissions of current CIA employees and contractors and to reflect current organizational titles, existing Board membership, and updated citations to certain applicable authorities.

Boldfaced text in this regulation indicates revisions.

(b)(3) CIAAct

This regulation was written by the Office of the Chief Information Officer,

2. (U//~~FOUO~~) AGENCY PREPUBLICATION REVIEW OF CERTAIN MATERIAL PREPARED FOR PUBLIC DISSEMINATION

(U//~~FOUO~~) SYNOPSIS. This regulation sets forth CIA policies and procedures for the submission and review of material proposed for publication or public dissemination by current and former employees and contractors and other individuals obligated by the CIA secrecy agreement to protect from unauthorized disclosure certain information they obtain as a result of their contact with the CIA. This regulation applies to all forms of dissemination, whether in written, oral, electronic, or other forms, and whether intended to be an official or nonofficial (that is, personal) publication.

- a. **(U//~~FOUO~~) AUTHORITY.** The National Security Act of 1947, as amended, the Central Intelligence Agency (CIA) Act of 1949, as amended, and Executive Order 12333, **as amended**, require the protection of intelligence sources and methods from unauthorized disclosure. Executive Order 13526, requires protection of classified information from unauthorized disclosure. 18 U.S.C. section 209 prohibits a federal employee from supplementation of salary from any source other than the U.S. Government as compensation for activities related to the employee's service as a Government employee. The *Standards of Ethical Conduct for Employees of the Executive Branch* (5 C.F.R. 2635) are the Government-wide ethics regulations that govern Federal employees. Those regulations include restrictions on outside activities and compensation for teaching, speaking, and writing related to official duties. In *Snepp v. U.S.*, 444 U.S. 507 (1980), the Supreme Court held that individuals who have been authorized access to CIA information, the public disclosure of which could harm the national security, hold positions of special trust and have fiduciary obligations to protect such information. These obligations are reflected in this regulation and in CIA secrecy agreements.

UNCLASSIFIED//~~AWO~~

b. (U//~~AWO~~) GENERAL REQUIREMENTS AND DEFINITIONS

- (1) The CIA requires all current and former Agency employees and contractors, and others who are obligated by CIA secrecy agreement, to submit for prepublication review to the CIA's Publications Review Board (PRB) all intelligence-related materials intended for publication or public dissemination, whether they will be communicated in writing, speeches, or any other method; and whether they are officially sanctioned or represent personal expressions, except as noted below.
- (2) The purpose of prepublication review is to ensure that information damaging to the national security is not disclosed inadvertently; and, for current employees and contractors, to ensure that neither the author's performance of duties, the Agency's mission, nor the foreign relations or security of the U.S. are adversely affected by publication.
- (3) The prepublication review requirement does not apply to material that is unrelated to intelligence, foreign relations, or CIA employment or contract matters (for example, material that relates to cooking, stamp collecting, sports, fraternal organizations, and so forth).
- (4) Agency approval for publication of nonofficial, personal works (including those of current and former employees and contractors and covered non-Agency personnel) does not represent Agency endorsement or verification of, or agreement with, such works. Therefore, consistent with cover status, authors are required, unless waived in writing by the PRB, to publish the following disclaimer:

"All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the Central Intelligence Agency (CIA) or any other U.S. Government agency. Nothing in the contents should be construed as asserting or implying U.S. Government authentication of information or CIA endorsement of the author's views. This material has been reviewed by the CIA to prevent the disclosure of classified information."

- (5) Those who are speaking in a nonofficial capacity must state at the beginning of their remarks or interview that their views do not necessarily reflect the official views of the CIA.
- (6) A nonofficial or personal publication is a work by anyone who has signed a CIA secrecy agreement (including a current and former employee or contractor), who has prepared the work as a private individual and who is not acting in an official capacity for the Government.
- (7) An official publication is a work by anyone who has signed a CIA secrecy agreement, (including a current employee or contractor), such as an article, monograph, or speech, that is intended to be unclassified and is prepared as part of their official duties as a Government employee or contractor acting in an official capacity.
- (8) "Publication" or "public dissemination" in this context means:
 - (a) for nonofficial (that is, personal) works -- communicating information to one or more persons; and
 - (b) for official works -- communicating information in an unclassified manner where that information is intended, or is likely to be, disseminated to the public or the media.
- (9) Covered non-Agency personnel means individuals who are obligated by a CIA secrecy agreement to protect from unauthorized disclosure certain information they obtain as a result of

UNCLASSIFIED//~~FOUO~~

their contact with the CIA.

c. (U//~~FOUO~~) THE PUBLICATIONS REVIEW BOARD

- (1) The PRB is the Agency body charged with reviewing, coordinating, and formally approving in writing all proposed nonofficial, personal publications that are submitted for prepublication. It is also responsible for coordinating the official release of certain unclassified Agency information to the public. The Board consists of a Chair and senior representatives from the Director of CIA Area, the National Clandestine Service (NCS), the Directorate of Support, the Directorate of Science and Technology, and the Directorate of Intelligence. **There is a nonvoting Executive Secretary and the Office of General Counsel (OGC) provides a nonvoting legal advisor.**
- (2) The PRB shall adopt and implement all lawful measures to prevent the publication of information that could damage the national security or foreign relations of the U.S. or adversely affect the CIA's functions or the author's performance of duties, and to ensure that individuals given access to classified information understand and comply with their contractual obligations not to disclose it. When the PRB reviews submissions that involve the equities of any other agency, the PRB shall coordinate its review with the equity-owning agency.
- (3) The PRB Chair is authorized unilaterally to represent the Board when disclosure of submitted material so clearly would not harm national security that additional review is unnecessary or when time constraints or other unusual circumstances make it impractical or impossible to convene or consult with the Board. The Chair may also determine that the subject of the material is so narrow or technical that only certain Board members need to be consulted.
- (4) During the course of PRB deliberations, the views of the equity-owning Board member regarding damage to national security and appropriateness for publication will be given great weight. In the even the PRB Chair and other Board members disagree as to whether the publication of information could damage the national security or if the *Studies in Intelligence* Editorial Board Chair disagrees with a PRB decision under section g(2) below that an article is inappropriate for publication, the PRB Chair, or Director of the Center for the Study of Intelligence, will have 15 days to raise the issue to the Chief, IMS for review, highlighting the equity-owner's concerns. If no resolution is reached at that level, the C/IMS will have 15 days to raise the matter to the Associate Deputy Director of the Central Intelligence Agency (ADD/CIA) for a final decision. When there is a disagreement whether information should be approved for publication, it will not be so approved until the issue is resolved by the C/IMS or the ADD/CIA. However, if the issue is not raised to the C/IMS or the ADD/CIA within the applicable time limits, the views of the equity-owning Board member will be adopted as the decision of the PRB (or in those cases where the *Studies of Intelligence* Editorial Board Chair disagrees with the PRB decision and the issue is not raised within applicable time limits, the PRB decision will be final).

d. (U//~~FOUO~~) CONTACTING THE PRB

- (1) Former employees and contractors and other covered non-Agency personnel must submit covered nonofficial (personal) materials intended for publication or public dissemination to the PRB by mail, fax, or electronically as follows:

For U.S. Mail:

CIA Publications Review Board



(b)(3) CIAAct

UNCLASSIFIED//AIUO

Washington, DC 20505

For Overnight Delivery (for example, FedEx, UPS, and so forth):

[Redacted box]

(b)(3) CIAAct

Facsimile: [Redacted box]

(b)(3) CIAAct

Email: [Redacted box]

(b)(3) CIAAct

Phone: [Redacted box]

(b)(3) CIAAct

- (2) Current employees and contractors must submit covered nonofficial and official materials intended for publication or public dissemination to the PRB by mail, fax, or electronically as follows:

Internal Mail: [Redacted box]

(b)(3) CIAAct

Classified Facsimile: [Redacted box]

(b)(3) CIAAct

Email: Lotus Note to: [Redacted box]

(b)(3) CIAAct

Secure Phone: [Redacted box]

(b)(3) CIAAct

- (3) Current employees and contractors intending to publish or speak on a nonofficial, personal basis must also complete and submit to the PRB an electronic cover memorandum identifying their immediate supervisor or contracting officer. The PRB will notify the appropriate Agency manager or contracting officer, whose concurrence is necessary for publication.

- (4) Review Timeline: As a general rule, the PRB will complete prepublication review for nonofficial publications within 30 days of receipt of the material. Relatively short, time-sensitive submissions (for example, op-ed pieces, letters to the editor, and so forth) will be handled as expeditiously as practicable. Lengthy or complex submissions may require a longer period of time for review, especially if they involve intelligence sources and methods issues. Authors are strongly encouraged to submit drafts of completed works, rather than chapters or portions of such works.

e. (U//~~AIUO~~) WHAT IS COVERED

- (1) Types of Materials. The prepublication review obligation applies to any written, oral, electronic, or other presentation intended for publication or public dissemination, whether personal or official, that mentions CIA or intelligence data or activities or material on any subject about which the author has had access to classified information in the course of his employment or other contact with the Agency. The obligation includes, but is not limited to, works of fiction; books; newspaper columns; academic journal articles; magazine articles; resumes or biographical information on Agency employees (submission to the PRB is the exclusive

UNCLASSIFIED//~~AWO~~

procedure for obtaining approval of proposed resume text); draft *Studies in Intelligence* submissions (whenever the author is informed by the *Studies* editor that the draft article is suitable for *Studies* Editorial Board review); letters to the editor; book reviews; pamphlets; scholarly papers; scripts; screenplays; internet blogs, e-mails, or other writings; outlines of oral presentations; speeches; or testimony prepared for a Federal or state or local executive, legislative, judicial, or administrative entity; and Officers in Residence (OIRs) speeches and publications (although oral and written materials prepared by OIRs exclusively for their classroom instructional purposes are not covered, OIRs must take particular care to ensure that any anecdotes or other classroom discussions of their Agency experiences do not inadvertently reveal classified information). Materials created for submission to the Inspector General and/or the Congress under the Whistleblower Protection Act and CIA implementing regulations are nonofficial, personal documents when they are initially created and the author is entitled to seek a review by the PRB to determine if the materials contain classified information and, if so, the appropriate level of classification of the information. If, at any point during or after the whistleblower process, the author wishes to disseminate his whistleblower complaint to the public, the author must submit his complaint to the PRB for full prepublication review under this regulation. If the author is a current employee or contractor who intends to disseminate his whistleblower complaint to the public, the author must also obtain PRB review of his materials under paragraph g below.

- (2) Review of Draft Documents. Written materials of a nonofficial, personal nature covered by the regulation must be submitted to the PRB at each stage of their development before being circulated to publishers, editors, literary agents, co-authors, ghost writers, reviewers, or the public (that is, anyone who does not have the requisite clearance and need-to-know to see information that has not yet been reviewed, but may be classified). This prepublication review requirement is intended to prevent comparison of different versions of such material, which would reveal the items that the Agency has deleted. For this reason, PRB review of material only after it has been submitted to publishers, reviewers, or other outside parties violates the author's prepublication review obligation. The Agency reserves the right to conduct a post-publication review of any such material in order to take necessary protective action to mitigate damage caused by such a disclosure. Such post-publication review and action does not preclude the U.S. Government or the CIA from exercising any other legal rights otherwise available as a result of this prepublication violation. Additionally, the Agency reserves the right to require the destruction or return to CIA of classified information found to have been included in earlier versions of a work regardless of the form of the media involved (for example, paper, floppy disk, hard disk, or other electronic storage methods).

(3) Public Presentations.

- (a) With respect to current and former employees and contractors and covered non-Agency personnel making intelligence-related speeches, media interviews, or testimony, they must submit all notes, outlines, or any tangible preparatory material to the PRB for review. Where no written material has been prepared specifically in contemplation of the speech, interview, or oral testimony, the individual must contact the PRB Chair or his representative to provide a summary of any and all topics that it is reasonable to assume may be discussed, and points that will or may be made. Unprepared or unrehearsed oral statements do not exempt an individual from possible criminal liability in the event they involve an unauthorized disclosure of classified information.
- (b) In addition, with respect to current employees and contractors making official or nonofficial oral intelligence-related statements to the media or to groups where the media will likely be

UNCLASSIFIED//~~AWO~~

in attendance, prior to granting interviews or making public appearances, the speaker shall contact the PRB for guidance. The PRB will coordinate the review of proposed speeches or media interviews with the component involved, the Office of Public Affairs for guidance regarding media or press relations, and other offices as necessary.

(c) Current employees who must make court appearances or respond to subpoenas must contact OGC for guidance.

(4) Official Publications. The publication or public dissemination of official Agency information by any means, including electronic transmissions, such as internet and unclassified facsimile, is subject to prepublication review. In addition to the types of materials listed in paragraph e(1) above, official publications subject to this review include unclassified monographs; organizational charts; brochures; booklets; flyers; posters; advertisements; films; slides; videotapes; or other issuances, irrespective of physical media such as paper, film, magnetic, optical, or electronic, that mention CIA or intelligence data or activities or material on any subject about which the author has had access to classified information in the course of his employment or other association with the Agency.

(5) Exclusions. Not included within the scope of this regulation are CIA court filings; regular, serial publications such as the *CIA World Fact Book*; or documents released pursuant to official declassification and release programs such as the Freedom of Information Act or the 25-Year Automatic Declassification Program under Executive Order 13526. Nor do these procedures apply to official documents intended to be disseminated only to other Federal Government entities (that is, responses to other Federal agencies and Congressional entities -- except for unclassified "constituent replies" that will remain covered by this regulation).

(6) Additional PRB Guidance. It is not possible to anticipate all questions that may arise about which materials require prepublication review. Therefore, it is the author's obligation to seek guidance from the PRB on all prepublication review issues not explicitly covered by this regulation.

f. ~~(U//AWO)~~ PREPUBLICATION REVIEW GUIDELINES FOR FORMER EMPLOYEES AND CONTRACTORS, AND COVERED NON-AGENCY PERSONNEL

(1) All material proposed for publication or public dissemination must be submitted to the PRB Chair, as described in paragraph d(1) above. The PRB Chair will have the responsibility for the review, coordination, and formal approval in writing of submissions in coordination with appropriate Board members. The PRB Chair will provide copies of submitted material to all components with equities in such material, and will also provide copies to all Board members and, upon request, to any Directorate-level Information Review Officer.

(2) The PRB will review material proposed for publication or public dissemination solely to determine whether it contains any classified information. Permission to publish will not be denied solely because the material may be embarrassing to or critical of the Agency. Former employees, contractors, or non-Agency personnel must obtain the written approval of the PRB prior to publication.

(3) When it is contemplated that a co-author who has not signed a CIA secrecy agreement will contribute to a publication subject to prepublication review, the final version of the publication must clearly identify those portions of the publication that were authored by the individual subject to the secrecy agreement. Where there is any ambiguity concerning which individual wrote a section, and the section was not submitted for review, the Agency reserves the right to

UNCLASSIFIED//~~AWO~~

consider the section to be entirely written by the individual subject to the secrecy agreement and therefore in violation of the individual's prepublication review obligations.

- (4) When otherwise classified information is also available independently in open sources and can be cited by the author, the PRB will consider the fact in making its determination on whether that information may be published with the appropriate citations. Nevertheless, the Agency retains the right to disallow certain open-source information or citations where, because of the author's Agency affiliation or position, the reference might confirm the classified content.

g. (U//~~AWO~~) PREPUBLICATION REVIEW GUIDELINES FOR CURRENT EMPLOYEES AND CONTRACTORS

- (1) All covered material proposed for publication or public dissemination must be submitted to the PRB Chair, as described in paragraph d(2) above. The PRB Chair will have the responsibility for the review, coordination, and formal approval in writing of submissions in coordination with the author's supervisor and other offices as necessary. The PRB Chair will provide copies of submitted material to all components with equities in such material, and will also provide copies to all Board members and, upon request, to any Directorate-level Information Review Officer.
- (2) Additional Review Criteria. Appropriateness. For current employees and contractors, in addition to the prohibition on revealing classified information, the Agency is also legally authorized to deny permission to publish any official or nonofficial materials on matters set forth in paragraphs e(1) and e(4) above that could:
- (a) reasonably be expected to impair the author's performance of his or her job duties,
 - (b) interfere with the authorized functions of the CIA, or
 - (c) have an adverse effect on the foreign relations or security of the United States.

These additional review criteria ensure that material is not published that could adversely affect the Agency's ability to function as an employer and carry out its national security mission. Because these criteria principally concern the Agency's authority as an employer to promote an effective work place and to protect the integrity of its mission, they apply only to the submissions of current CIA employees and contractors.

When a current CIA officer engages in public discussion of internal organizational operations, policies, and information, it could in certain circumstances interfere with CIA's ability, as an employer, to promote an effective work place and carry out its mission. When a current CIA officer engages in public discussion of current foreign relations issues or intelligence-related matters, it could in certain circumstances provide a factual basis for some to reasonably question whether the CIA was properly carrying out its independent, objective, and apolitical intelligence functions.

The determination of whether any particular publication could impair the author's performance of his or her duties, interfere with authorized CIA functions, or adversely affect the foreign relations or security of the United States must be assessed case-by-case in terms of the content of the manuscript, as well as the overall context and prevailing circumstances, including but not limited to, consideration of the currency of the subject matter; whether the subject matter is a matter of public concern; the degree

UNCLASSIFIED//~~AWO~~

to which the topic is related to the author's official duties; whether the material submitted for review is required for a course at an accredited U.S. educational institution at any academic level and, if so, whether distribution is intended to extend beyond classroom use; and whether, in light of the assignment in which the author serves, the inclusion or exclusion of the disclaimer described in paragraph b(4) above can mitigate any concerns. The Agency will exercise its authority to deny permission to publish on the basis of any such determination only when the determination is made in writing and clearly identifies or describes how publication could create a significant risk of impairing the author's performance of his or her job duties, interfering with the authorized functions of the CIA, or adversely affecting the foreign relations or security of the United States.

Prior to drafting a manuscript intended for nonofficial publication, current CIA officers are encouraged to consult with the Board regarding the proposed topic or subject matter. In addition, current CIA officers must comply with any applicable component policies and procedures relating to consultation with management prior to the drafting of a manuscript, prior to submitting a manuscript to the Board, or during the prepublication review process. Any consultation with the Board or management may not necessarily result in Agency approval to publish the submitted manuscript.

- (3) Outside Activities Approval Request. Current employees and contractors must also complete a Form 879 (Outside Activity Approval Request) in accordance with Agency Regulation 10-15.

(4) Review Process:

(a) Nonofficial publications. For all nonofficial publications, current employees must complete and submit to the PRB a cover memorandum identifying their immediate supervisor or contracting officer. The PRB will notify these individuals, whose concurrence is necessary for publication.

(b) Unclassified official publications. For all unclassified official publications that are covered by this regulation, current employees or contractors must first coordinate the document or speech with their management chain. Once initial management acceptance has been made, the employee must then submit the **proposed** publication to the PRB for final review and approval. (*Classified* official publications are not covered by this regulation and, therefore, are not required to be submitted to the PRB for review.)

(c) Resumes. This requirement for management review and concurrence does not apply for resumes, which must be sent to the PRB, which will coordinate their approval with the appropriate equity-owning component and Directorate-level Information Review Officer. The employee must obtain the written approval of the PRB prior to any dissemination of the resume outside of the CIA.

- (5) OGC Ethics Review for Executive Branch Employees. As part of the prepublication review process, and after PRB/management review of proposed publications is completed, the PRB will initiate a further review by OGC/Ethics Law Division (**OGC/ELD**) to determine if any ethics issues are raised under the *Standards of Ethical Conduct for Employees of the Executive Branch*. These Government-wide regulations and Agency Regulation 13-2 limit the use of nonpublic information and provide that an employee shall not receive compensation from any source other than the Government for teaching, speaking, or writing relating to the

UNCLASSIFIED//~~AWO~~

employee's official duties. Additionally, OGC/ELD will also review proposed publications by current employees to ensure there is no violation of the criminal statute, 18 U.S.C. section 209, which prohibits an employee from receiving any salary or any contribution to or supplementation of salary from any source other than the U.S. as compensation for services as a Government employee. Specifically, employees may not receive outside compensation for any article, speech, or book written or produced as part of their official duties.

h. (U//~~AWO~~) APPEALS

- (1) If the PRB denies all or part of a proposed nonofficial publication, the author may submit additional material in support of publication and request reconsideration by the PRB. In the event the PRB denies the request for reconsideration, the author may appeal. PRB decisions involving nonofficial publications may be appealed to the ADD/CIA within 30 days of the decision. Such an appeal must be in writing and must be sent to the PRB Chair. Appeal documentation must include the material intended for publication and any supporting materials the appealing party wishes the ADD/CIA to consider. The PRB Chair will forward the appeal and relevant documentation through the components that objected to publication of the writing or other product at issue. The Director or Head of Independent Office will affirm or recommend revision of the decision affecting his or her component's equities and will forward that recommendation to OGC. OGC will review the recommendations for legal sufficiency and will make a recommendation to the ADD/CIA for a final Agency decision. The PRB Chair is responsible for staff support to the ADD/CIA. The ADD/CIA will render a written final decision on the appeal. Best efforts will be made to complete the appeal process within 30 days from the date the appeal is submitted.
- (2) This regulation is intended to provide direction and guidance for those persons who have prepublication review obligations and those who review material submitted for nonofficial or official publication. Nothing contained in this regulation or in any practice or procedure that implements this regulation is intended to confer, or does confer, any substantive or procedural right of privilege on any person or organization beyond that expressly stated herein.

- i. **(U//~~AWO~~) BREACH OF SECRECY AGREEMENT.** Failure to comply with prepublication review obligations can result in the imposition of civil penalties or damages. When the PRB becomes aware of a potential violation of the CIA secrecy agreement, it will notify OGC and the Office of Security (OS). After the OS review and investigation of the case is completed, if further action is deemed warranted, the OS will refer the matter to OGC, which will report all potentially criminal conduct to the Department of Justice (DoJ) and consult with DoJ regarding any civil remedies that may be pursued.



Department of Defense INSTRUCTION

NUMBER 5230.29

August 13, 2014

Incorporating Change 1, April 14, 2017

DCMO

SUBJECT: Security and Policy Review of DoD Information for Public Release

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5105.53 (Reference (a)), *DoDD 5105.82 (Reference (b))*, and Deputy Secretary of Defense Memorandum (Reference (bc)), this instruction reissues DoD Instruction (DoDI) 5230.29 (Reference (ed)) to implement policy established in DoDD 5230.09 (Reference (de)), assigns responsibilities, and prescribes procedures to carry out security and policy review of DoD information for public release.

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

b. Does not apply to the Office of the Inspector General of the Department of Defense. The Inspector General of the Department of Defense, as an independent and objective officer in the DoD, is exempt from the policy review provisions of this instruction. As necessary, information may be submitted for security review before public release.

3. POLICY. In accordance with Reference (de), it is DoD policy that a security and policy review will be performed on all official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the DoD.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. Enclosure 3 contains clearance requirements, submission procedures, time limits, information concerning review determinations, and appeals.

DoDI 5230.29, August 13, 2014

6. RELEASABILITY. **Cleared for public release.** This instruction is available on the **Internet** ~~from the~~ DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

7. EFFECTIVE DATE. This instruction ~~is~~ *is effective August 13, 2014.*

~~a. Is effective August 13, 2014.~~

~~b. Will expire effective August 13, 2024 if it hasn't been reissued or cancelled before this date in accordance with DoDI 5025.01 (Reference (e)).~~



David Tillotson III
Assistant Deputy Chief Management Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

Change 1, 04/14/2017

DoDI 5230.29, August 13, 2014

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5105.53, "Director of Administration and Management (DA&M)," February 26, 2008
- (b) *DoD Directive 5105.82, "Deputy Chief Management Officer (DCMO) of the Department of Defense," October 17, 2008*
- (bc) Deputy Secretary of Defense Memorandum, "Reorganization of the Office of the Deputy Chief Management Officer," July 11, 2014
- (ed) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009 (hereby cancelled)
- (de) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended
- ~~(e) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014~~
- (f) DoD Instruction 5400.04, "Provision of Information to Congress," March 17, 2009
- (g) DoD Instruction 5230.24, "Distribution Statements on Technical Documents," August 23, 2012, *as amended*
- (h) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, as amended
- (i) Parts 120-130 of Title 22, Code of Federal Regulations (also known as "The International Traffic in Arms Regulations (ITAR)")
- (j) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
- (k) DoD Manual 5200.01, "DoD Information Security Program," *February 24, 2012, as amended date varies by volume*
- (l) Deputy Secretary of Defense Memorandum, "Congressional Testimony Coordination and Clearance Procedures," January 17, 2012¹
- (m) DoD Instruction 2205.02, "Humanitarian and Civic Assistance (HCA) Activities," June 23, 2014
- (n) DoD Instruction 3000.05, "Stability Operations," September 16, 2009
- (o) DoD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," September 5, 2008
- (p) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
- (q) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," *October 6, 1987-November 18, 2016*
- (r) DoD Instruction 3200.12, "DoD Scientific and Technical Information Program (STIP)," August 22, 2013
- (s) DoD Manual 3200.14, Volume 1, "Principles and Operational Parameters of the DoD Scientific and Technical Information Program (STIP): General Processes," March 14, 2014

¹ Available at <http://www.dtic.mil/whs/esd/osr>

DoDI 5230.29, August 13, 2014

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR OF ADMINISTRATION, OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER (DCMO) OF THE DEPARTMENT OF DEFENSE (DA ODCMO). Under the authority, direction, and control of the ~~Deputy Chief Management Officer (DCMO) of the Department of Defense~~, the ~~Director of Administration DA ODCMO~~ acts as the appellate authority for the DoD security and policy review process.

2. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). Under the authority, direction, and control of the DCMO, through the ~~Director of Administration DA ODCMO~~, the Director, WHS:

a. Monitors compliance with the procedures established in Enclosure 3 of this instruction for the security and policy review of official DoD information.

b. Provides for the timely security and policy review of official DoD information proposed for public release that is originated by, in, or for the DoD, including statements intended for open presentation before the Congress and other material submitted to the Congress in accordance with DoDI 5400.04 (Reference (f)).

c. Provides for the timely policy review of official DoD information that is originated by the DoD for presentation before a closed session of the Congress and other classified material submitted to the Congress in accordance with Reference (f).

d. Coordinates, as necessary, with the DoD Component staffs when reviewing official DoD information for public release clearance to ensure accuracy and currency of existing policy and security guidance.

e. Responds to requests for review of information submitted by DoD personnel acting in a private capacity or submitted voluntarily by non-DoD sources to ensure that classified information is not disclosed. This review will also address technology transfer and public releasability of technical data in accordance with DoDI 5230.24, DoDD 5230.25, and parts 120 through 130 of Title 22, Code of Federal Regulations (References (g), (h), and (i)).

f. Supports other Executive Department and non-DoD agency security review programs in the release of information to the public that may contain DoD equities.

3. OSD AND DOD COMPONENT HEADS. The OSD and DoD Component heads:

a. Ensure Component compliance with this instruction, and issue any guidance necessary for the internal administration of the requirements prescribed in Enclosure 3 of this instruction.

Change 1, 04/14/2017

DoDI 5230.29, August 13, 2014

b. Ensure prompt Component guidance and assistance to the Chief, Defense Office of Prepublication and Security Review (DOPSR), when requested, on any information proposed for public release.

c. Exercise Component clearance authority for information not specified in section 1 of Enclosure 3 of this instruction. This authority may be delegated to the lowest level competent to evaluate the content and implications of public release of the information.

d. Ensure that Component-specific documents, including official correspondence, are reviewed internally and that information not specified in Enclosure 3 of this instruction is reviewed for operations security and information security in accordance with DoDD 5205.02E and DoD Manual 5200.01 (References (j) and (k)) before public release. This review will also address technology transfer and public releasability of technical data in accordance with References (g), (h), and (i).

e. Ensure Component compliance with the guidelines of the Deputy Secretary of Defense Memorandum (Reference (l)) concerning the coordination and clearance process of Congressional testimony to facilitate timely security and policy review.

f. Ensure effective information sharing between the Component and designated mission partners in accordance with DoDI 2205.02 and DoDI 3000.05 (References (m) and (n)).

g. Ensure that Component release of DoD information to news media representatives is in accordance with DoDD 5122.05 (Reference (o)).

DoDI 5230.29, August 13, 2014

ENCLOSURE 3

PROCEDURES

1. CLEARANCE REQUIREMENTS. The security review protects classified information, controlled unclassified information, or unclassified information that may individually or in aggregate lead to the compromise of classified information or disclosure of operations security. The policy review ensures that no conflict exists with established policies or programs of the DoD or the U.S. Government. Official DoD information that is prepared by or for DoD personnel and is proposed for public release will be submitted for review and clearance if the information:

- a. Originates or is proposed for release in the National Capital Region by senior personnel (e.g., general or flag officers and Senior Executive Service) on sensitive political or military topics;
- b. Is or has the potential to become an item of national or international interest;
- c. Affects national security policy, foreign relations, or ongoing negotiations;
- d. Concerns a subject of potential controversy among the DoD Components or with other federal agencies;
- e. Is presented by a DoD employee who, by virtue of rank, position, or expertise, would be considered an official DoD spokesperson; or
- f. Contains technical data, including data developed under contract or independently developed and subject to potential control in accordance with Reference (i), that may be militarily critical (as defined in the Glossary) and subject to limited distribution, but on which a distribution determination has not been made.

2. SUBMISSION PROCEDURES

a. Detailed Procedures. These procedures apply to all information required to be submitted to DOPSR for clearance:

(1) A minimum of three hard copies of material, in its final form, will be submitted, together with a signed DD Form 1910, "Clearance Request for Public Release of Department of Defense Information," located at the DoD Forms Management Program website at <http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>, to:

Chief, Defense Office of Prepublication and Security Review
1155 Defense Pentagon
Washington, D.C. 20301-1155

DoDI 5230.29, August 13, 2014

(2) If the material is fewer than 100 pages long, one soft copy of the unclassified material and the DD Form 1910 may be submitted by e-mail to whs.pentagon.esd.mbx.secrev@mail.mil instead of the requirements of paragraph 2a(1) of this enclosure.

(3) Any material submitted for review will be approved by an authorized government representative of the submitting office to indicate that office's approval of the material for public release. Contractors may not sign the DD Form 1910.

(4) All information submitted for clearance to DOPSR must first be coordinated within the originating DoD Component to ensure that it:

- (a) Reflects the organization's policy position.
- (b) Does not contain classified, controlled unclassified, or critical information requiring withholding.
- (c) Is reviewed for operations security in accordance with References (j) and (k).
- (d) Is reviewed to ensure there is no risk of releasing classified, controlled unclassified, operations security, or critical information if the information is aggregated with other publicly available data and information in accordance with References (j) and (k).

(5) Only the full and final text of material proposed for release will be submitted for review. Drafts, notes, outlines, briefing charts, etc., may not be submitted as a substitute for a complete text. DOPSR reserves the right to return draft or incomplete documents without action.

(6) Abstracts to be published in advance of a complete paper, manuscript, etc., require clearance. Clearance of an abstract does not fulfill the requirement to submit the full text for clearance before its publication. If an abstract is cleared in advance, that fact, and the DOPSR case number assigned to the abstract, will be noted on the DD Form 1910 or other transmittal when the full text is submitted.

b. Other Requirements. The requirements of References (f) and (l) will apply to the processing of information proposed for submission to Congress.

c. Website Publication. Information intended for placement on websites or other publicly accessible computer servers that are available to anyone requires review and clearance for public release if it meets the requirements of section 1 of this enclosure and DoDI 8550.01 (Reference (p)). Website clearance questions should be directed to the Component's website manager. Review and clearance for public release is not required for information to be placed on DoD controlled websites or computer servers that restrict access to authorized users.

d. Basic Research. Submitters will comply with the DoD guidance on basic scientific and technical research review in DoDI 5230.27 (Reference (q)).

DoDI 5230.29, August 13, 2014

e. Federally Funded Research and Engineering. Submitters will comply with the DoD guidance in federally funded research and engineering in DoDI 3200.12 and DoDI 3200.14 (References (r) and (s)), which requires submitters to send the final published document or final author's referenced manuscript to the Defense Technical Information Center (DTIC).

3. TIMELINES FOR SUBMISSION

a. Prepublication Security and Policy Review Requests

(1) Submit speeches and briefings to DOPSR at least 5 working days before the event at which they are to be presented. Additional time may be needed for complex or potentially controversial speeches due to coordination requirements.

(2) Other material (e.g., papers and articles) will be submitted to DOPSR at least 10 working days before the date needed. The length, complexity, and content will determine the number of agencies required to review the document and, consequently, the time required for the complete review process.

(3) Technical papers will be submitted to DOPSR at least 15 working days before the date needed. More time may be needed if DOPSR determines that the material is complex or requires review by agencies outside of the DoD.

(4) Manuscripts and books will be submitted to DOPSR at least 30 working days before the date needed and before submission to a publisher. More time may be needed if DOPSR determines that the material is complex or requires review by agencies outside of the DoD.

(5) DOPSR reserves the right to return documents without action if insufficient time is allowed for prepublication review.

b. Congressional Security and Policy Review Requests. Security and policy review of material submitted by the DoD to Congress will be provided to DOPSR in these timeframes to allow for a thorough review for DoD to comply with the congressional committee or subcommittee mandates:

(1) Statements: 5 days before submission to the DoD Office of Legislative Counsel in accordance with References (f) and (l).

(2) A minimum of 5 working days for these requests:

(a) Questions for the Record.

(b) Inserts for the Record.

(c) Advance Policy Questions.

DoDI 5230.29, August 13, 2014

- (d) Selected Acquisition Reports.
- (e) Budget documents (in accordance with Reference (f)).
- (f) Classified transcripts only (in accordance with Reference (f)).
- (g) Reprogramming actions.
- (h) Congressional reports.

4. REVIEW DETERMINATIONS AND APPEALS

a. General. Information reviewed for release to the public will result in one of these determinations:

(1) Cleared for Public Release. The information may be released without restriction by the originating DoD Component or its authorized official. DOPSR may require a disclaimer to accompany the information, as follows: "The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government."

(2) Cleared "With Recommendations" for Public Release. Optional corrections, deletions, or additions are included. Although DOPSR has no responsibility for correcting errors of fact or making editorial changes, obvious errors may be identified in the text and noted as "recommended." These corrections are not binding on the author or submitter.

(3) Cleared "As Amended" for Public Release. Amendments, made in red, are binding on the submitter. Red brackets identify information that must be deleted. If the amendments are not adopted, then the DoD clearance is void. When possible, alternative wording is provided to substitute for the deleted material. Occasionally, wording will be included that must be added to the text before public release. A disclaimer, as shown in paragraph a(1) of this section, may also be required.

(4) Not Cleared for Public Release. The information submitted for review may not be released.

b. Appeals. All amendments or "not cleared" determinations may be appealed in writing by the requester within 60 days to DOPSR. The appeal must contain the basis for release of information denied during the initial determination. All appeals will be resolved at the lowest practical level and as quickly as possible. In accordance with Reference (a), the ~~Director of Administration~~ *DA ODCMO* serves as the appellate authority for any denials or redactions that may be contested. When the appellate authority makes a final determination, a written response will be promptly forwarded to the requester.

DoDI 5230.29, August 13, 2014

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

<i>DA ODCMO</i>	<i>Director of Administration, Office of the Deputy Chief Management Officer of the Department of Defense</i>
DCMO	Deputy Chief Management Officer <i>of the Department of Defense</i>
DoDD	DoD directive
DoDI	DoD instruction
DOPSR	Defense Office of Prepublication and Security Review
WHS	Washington Headquarters Services

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this instruction.

authorized government representative. A government employee who possesses the authority to communicate a particular component's policies and recommendation for public release.

militarily critical. Information will be considered militarily critical if it addresses any of these subjects or affects the operations security thereof:

New weapons or weapons systems, or significant modifications or improvements to existing weapons or weapons systems, equipment, or techniques.

Military operations and significant exercises of national or international significance.

Command, control, communications, computers, intelligence, surveillance, and reconnaissance; information operations and cyberspace; weapons of mass destruction; improvised explosive devices; and computer security.

Military activities or application in space; nuclear weapons, including nuclear weapons effects research; defense from chemical and biological warfare and threats; initial fixed weapons basing; and arms control treaty implementation.

Any other contemporary topic that is designated by the DoD Component head.

public release. The act of making information available to the public with no restrictions on access to or use of the information. Authorization and release of information to the public, cleared by DOPSR, is the responsibility of the originating office.

DIVISION N – INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2017

The following is the explanation of the Intelligence Authorization Act for Fiscal Year 2017.

This explanation reflects the status of negotiations and disposition of issues reached between the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence (hereinafter, “the Agreement”). The explanation shall have the same effect with respect to the implementation of this Act as if it were a joint explanatory statement of a conference committee.

The explanation comprises three parts: an overview of the application of the annex to accompany this statement; unclassified congressional direction; and a section-by-section analysis of the legislative text.

PART I: APPLICATION OF THE CLASSIFIED ANNEX

The classified nature of U.S. intelligence activities prevents the congressional intelligence committees from publicly disclosing many details concerning the conclusions and recommendations of the Agreement. Therefore, a classified Schedule of Authorizations and a classified annex have been prepared to describe in detail the scope and intent of the congressional intelligence committees’ actions. The Agreement authorizes the Intelligence Community (IC) to obligate and expend funds not altered or modified by the classified Schedule of Authorizations as requested in the President’s budget, subject to modification under applicable reprogramming procedures.

The classified annex is the result of negotiations between the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. It reconciles the differences between the committees’ respective versions of the bill for the National Intelligence Program (NIP) and the Homeland Security Intelligence Program (HSIP) for Fiscal Year 2017. The Agreement also makes recommendations for the Military Intelligence Program (MIP), and the Information Systems Security Program (ISSP), consistent with the National Defense Authorization Act for Fiscal Year 2017, and provides certain direction for these two programs.

The Agreement supersedes the classified annexes to the reports accompanying: H.R. 5077, as passed by the House on May 24, 2016; H.R. 6393, as passed by the House on November 20, 2016; H.R. 6480, as passed by the House on December 8, 2016; S. 3017, as reported by the Senate Select Committee on Intelligence on June 6, 2016; and S. 133, as reported by the Senate Select Committee on Intelligence on January 20, 2017. All references to the House-passed and Senate-reported annexes are solely to identify the heritage of specific provisions.

The classified Schedule of Authorizations is incorporated into the bill pursuant to Section 102. It has the status of law. The classified annex supplements and adds detail to clarify the authorization levels found in the bill and the classified Schedule of Authorizations. The classified annex shall have the same legal force as the report to accompany the bill.

PART II: SELECT UNCLASSIFIED CONGRESSIONAL DIRECTION

Managing intelligence community personnel

This Agreement by the congressional intelligence committees accepts the Senate's recommendations that IC elements should build, develop, and maintain a workforce appropriately balanced among its civilian, military and contractor workforce sectors to meet the missions assigned to it in law and by the president. The Agreement recognizes that the size and shape of the IC's multi-sector workforce should be based on mission needs, and encourages the IC to adjust its reliance on contractors when appropriate, both as a matter of general policy and as a way to conserve resources. The flexibility afforded in this provision should support this position. In addition, section 103 provides an increase in the number of civilian personnel authorized in the Schedule of Authorizations for the purposes of such contractor conversions in the interim for the remainder of fiscal year 2017. Nothing precludes the Congress from addressing the end strength for any element or office of the IC in the annual authorization bills.

Therefore, the committees direct that the ODNI provide the congressional intelligence committees briefings on the workforce initiative as directed in section 306, beginning July 1, 2017, and each 120 days thereafter until July 1, 2018, with benchmarks and milestones, for IC elements to manage a multi-sector workforce without personnel ceilings starting in fiscal year 2019. The ODNI, in coordination with the IC elements, shall establish a common methodology for collecting and reporting data, and include new exhibits in the annual congressional budget justification books that display full-time equivalents (government civilians, core contractors, non-core contractors, and military personnel), by program, expenditure center and project.

In the absence of authorized position ceiling levels, agencies will be bound to authorized and appropriated personal services funding levels.

Further, the transfer of non-personal services funding in below-threshold reprogramming is a concern to the committees. Therefore, the committees direct agencies to provide a written notification to the committees of any realignment and/or reprogramming of funding between personal services and non-personal services.

Commercial Geospatial Intelligence Strategy

The congressional intelligence committees applaud the National Geospatial-Intelligence Agency (NGA) for issuing its October 2015 Commercial Geospatial Intelligence (GEOINT) Strategy, which states a goal of fostering a "more diverse, resilient, agile, and responsive GEOINT program that provides seamless user access to the best mix of commercial GEOINT . . . to fulfill National System for Geospatial-Intelligence (NSG) and Allied System for Geospatial-Intelligence (ASG) mission needs." The committees also find merit in the NGA's "GEOINT Pathfinder" project, which seeks to maximize the use of unclassified and commercially available data sources that can be easily and rapidly shared with a variety of military, United States and allied government, and non-government customers, and supports the project's continuation and expansion.

The committees further commend the NGA for pursuing new methods of intelligence collection and analysis to inform, complement, and add to its support of warfighter requirements by looking to emerging commercial technology providers, including small satellite companies, which hold the promise of rapid technological innovation and potentially significant future cost savings to the U.S. taxpayer. The committees further encourage the Director of the NGA to ensure sufficient funding is available to acquire new, unclassified sources, including commercial satellite imagery providing unprecedented global persistence, as well as products and services that provide information and context about changes relevant to geospatial intelligence. The committees also encourage the NGA to pursue new business models, including commercial acquisition practices, to enable the NGA's access to data, products, and services in ways consistent with best commercial practices.

The committees fully support the NGA's course of action in partnering with the commercial GEOINT industry to meet future warfighter intelligence requirements, while recognizing the need to take appropriate steps to protect national security, and encourage the Director of the NGA and the Under Secretary of Defense for Intelligence to keep the committees informed of their progress in implementing this strategy. Therefore, this Agreement directs the Department of Defense (DoD), in building future-year budgets, to ensure continued funding is provided for implementation, through at least Fiscal Year 2021, of the Commercial Geospatial Intelligence Strategy issued by the NGA in October 2015.

Space Launch Facilities

The congressional intelligence committees continue to believe it is critical to preserve a variety of launch range capabilities to support national security space missions. Spaceports or launch and range complexes may provide capabilities to reach mid-to-low or polar-to-high inclination orbits. The committees believe an important component of this effort may be state-owned and operated spaceports that are commercially licensed by the Federal Aviation Administration, which leverage non-federal public and private investments to bolster U.S. launch capabilities. Additionally, the committees believe that these facilities may be able to provide additional flexibility and resilience to the Nation's launch infrastructure, especially as the nation considers concepts such as the reconstitution of satellites to address the growing foreign counterspace threat. The committees note recent testimony by the Chief of Staff of the U.S. Air Force, General Mark Welsh, who stated,

As we look at this space enterprise and how we do it differently in the future, as we look more at disaggregation, microsats, cube sats, small sats, things that don't have to go from a large launch complex all the time, I think proliferating launch complexes is probably going to be a natural outshoot of this. I think it's commercially viable, it may be a way for companies to get into the launch business who could not afford to get into it or don't see a future in it and for large national security space launches, but I think this has got to be part of the strategy that this whole national team puts together as we look to the future.

Therefore, the Agreement directs the IC, in partnership with the U.S. Air Force, to consider the role and contribution of spaceports or launch and range complexes to our national security space launch capacity, and directs the Office of the Director of National Intelligence, in

consultation with the Department of Defense and the U.S. Air Force, to brief the congressional intelligence committees on their plans to utilize such facilities within 90 days of enactment of this Act.

National Reconnaissance Office Workforce Optimization Strategy

The congressional intelligence committees have had longstanding interest in, and support for, a permanent government cadre to provide the National Reconnaissance Office (NRO) with a stable, expert acquisition workforce. The committees applaud the substantial progress that the NRO has made in the past year in this regard. The committees have parallel interests in providing the IC with flexibility to manage a multi-sector workforce and in continuing the reduction in the reliance on contractors.

Therefore, the Agreement directs the NRO to conduct a workforce review to optimize the mix between government civilians and contractors and report to the committees with a strategy within 90 days of enactment of this Act.

Guidance and reporting requirement regarding interactions between the intelligence community and entertainment industry.

The congressional intelligence committees believe that there are important, valid reasons for elements of the IC to engage with the entertainment industry, among other things to ensure the correction of inaccuracies, demonstrate the IC's commitment to transparency, and to ensure that the IC recruits and retains highly qualified personnel to the fullest extent possible. The committees further believe that IC engagement with the entertainment industry should be conducted in the most cost effective and deliberate fashion possible, while ensuring that classified information is protected from unauthorized disclosure.

These engagements – some of which have been described in partially-declassified inspector general reports – cost taxpayer dollars, raise potential ethics concerns, increase the risk of disclosure of classified information, and consume the time and attention of IC personnel responsible for United States national security. Neither the production of entertainment nor the self-promotion of IC entities are legitimate purposes for these engagements.

Review of the National Intelligence University

The National Intelligence University (NIU) has made significant progress in recent years in its transition from a defense intelligence college to a national intelligence university that provides advanced education in a classified format. Such advanced education is integral to making intelligence a profession with recognized standards for performance and ethics and fostering an integrated IC workforce. While progress has been significant since the Director of National Intelligence (DNI) and Secretary of Defense agreed to redesignate Defense Intelligence Agency's (DIA) National Defense Intelligence College as NIU in 2011, the institution must continue to adapt to functioning as a university with a robust research agenda, and to serving the entire IC, not just elements of DoD.

Fiscal years 2017 and 2018 are of great significance for NIU, as it moves its principal facility to the IC Campus at Bethesda, completes activities associated with its 2018 decennial regional accreditation reaffirmation, and receives a new president. The congressional intelligence committees believe that these developments position NIU to make further progress in its vision to become the center of academic life for the IC.

To guide these next steps, the Agreement directs DIA, in coordination with ODNI and the Office of the Under Secretary of Defense for Intelligence, to, no later than 30 days after enactment of this Act, select a five member, external, and independent panel to conduct a review of NIU. The panel shall submit a report detailing the results of such review to the congressional intelligence and defense committees within 180 days of enactment of this Act. The panel should be composed of recognized academics, personnel from other DoD joint professional military education institutions, national security experts, and at least one member of NIU's Board of Visitors.

This review and the resulting report shall, among other things, assess:

- (1) Methods for ensuring a student body that is more representative of all IC elements;
- (2) Incentives for IC elements to send personnel to NIU to earn a degree or certificate, to include designating attendance at NIU as positions reimbursable by ODNI and requiring IC elements to employ the workforce concept of "float" for personnel enrolled in higher-education programs;
- (3) How certificate programs align with NIU's unique value as an institution of advanced intelligence education;
- (4) Methods to enhance NIU's research program, to include publication of a journal, hosting of conferences and other collaborative fora, and more formalized relationships with intelligence studies scholars;
- (5) Whether and how educational components of other IC elements could provide educational offerings as part of the NIU curriculum;
- (6) Potential advantages and risks associated with alternative governance models for NIU, to include moving it under the auspices of ODNI; and
- (7) The feasibility and resource constraints of NIU tailoring degree offerings to meet the needs of IC personnel at different stages in their careers, similar to DoD's joint professional military education model.

Cost of living consideration

The congressional intelligence committees are concerned with the high cost of living for military, civilian, and contractor personnel at overseas Combatant Command intelligence centers. Although the committees recognize the benefits of co-locating intelligence analysts with

the operational commander, the intelligence centers for both U.S. European Command (USEUCOM) and U.S Africa Command (USAFRICOM) are located over 600 miles from their Combatant Command headquarters. Combatant Commanders based in the United States regularly communicate with forward deployed units, and the USEUCOM and USAFRICOM intelligence centers have developed mechanisms to effectively employ various teleconferencing and virtual communication tools to ensure collaboration across large distances.

The congressional intelligence committees are concerned that despite the utility of these virtual collaboration tools, DoD has not taken action to reduce the number of intelligence personnel stationed in high cost of living areas. These costs can exceed \$65,000 per person, per year in annual cost of living allowances compared to the continental United States (CONUS) expenses. The additional costs associated with stationing intelligence personnel in high-cost overseas locations detract from other critical intelligence priorities. The committees are further concerned that DoD does not adequately account for the long-run expense of high costs of living when selecting locations for intelligence facilities.

Therefore, the Agreement directs the DIA to evaluate alternate mechanisms for staffing overseas Combatant Command intelligence centers, particularly those that are not co-located with Combatant Command headquarters, and to identify cost-savings opportunities by shifting personnel to lower cost locations, including in the continental United States.

Defense Intelligence Agency education opportunities

DIA presently allows DIA employees to receive pay for a single year only while attending certain graduate degree programs on a full-time basis. Employees may pursue such opportunities at the National Intelligence University and similar institutions; and, in certain circumstances, also at public and private civilian universities. However, the one-year limit discourages DIA personnel from pursuing multi-year graduate degree programs. Expanding DIA's program to allow highly qualified DIA employees to pursue multi-year graduate degree programs from accredited civilian universities would further improve retention, recruitment, and foster diversity of thought at DIA.

Therefore, the Agreement directs DIA, no later than 180 days after the enactment of this Act, to:

(1) Provide for and fund a program that allows for DIA employees to attend civilian graduate degree programs for up to two years each, based on the standard length of the relevant program, provided that:

(a) Where DIA deems appropriate, employees may pursue academic programs extending beyond two years. Consistent with current practices, the program should be made available to at least five employees each year, with each employee receiving a full-time salary while participating in the program; and

(b) Each DIA participant shall be subject to any program approvals, service obligations, repayment obligations, and other requirements pertaining to academic programs, as prescribed by applicable laws and policies.

(2) Brief the congressional intelligence committees on the status of the program's implementation.

Mental health prevalence

The congressional intelligence committees are committed to supporting the men and women of the IC, who bravely risk their lives serving their country as civilians in conflict zones and other dangerous locations around the world. These individuals often serve next to their military counterparts in areas of active hostilities. As such, they are often exposed to many of the emotional stresses generally associated with a tour of duty abroad. The committees believe there are deficiencies and inconsistencies in the pre- and post-deployment mental health and wellness services available to civilian employees.

Therefore, the Agreement directs the National Security Agency (NSA), NGA, the Central Intelligence Agency (CIA), and DIA, no later than 180 days after the enactment of this Act, to provide a joint briefing to the congressional intelligence committees on the mental health screenings and related services that these agencies offer employees, both before and after they deploy to combat zones. Such briefing shall include a description of:

- (1) Existing services available;
- (2) Agency resources for and analysis of these services, including the frequency of use by employees compared to the total number returning from deployment; and
- (3) How agencies with deployed civilian employees are sharing best practices and leveraging services or resources outside their agencies.

Review of the Office of the Director of National Intelligence

It has been more than ten years since the Congress established the position of the Director of National Intelligence (DNI) in the Intelligence Reform and Terrorism Prevention Act of 2004, building on its predecessor, the Director of Central Intelligence. Given this experience and the evolving security environment, the committees believe it appropriate to review the DNI's roles, missions and functions and adapt its authorities, organization and resources as needed.

Therefore, the Agreement directs the President to form an independent, external panel of at least five individuals with significant intelligence and national security expertise to review ODNI's roles, missions and functions and make recommendations, as needed, regarding its authorities, organization and resources. The panel shall:

- (1) Evaluate ODNI's ability to fulfill the responsibilities assigned to it in law given its current scope and structure;

- (2) Assess whether any roles and responsibilities currently assigned to the DNI could be more effectively or efficiently executed by other IC components or government agencies outside the IC;
- (3) Analyze the personnel, funding, and authorities required for each component of ODNI to perform each of its assigned responsibilities;
- (4) Evaluate the organizational structure of ODNI;
- (5) Review the size, role, purpose and function of ODNI's mission centers;
- (6) Assess the value of the national intelligence manager construct;
- (7) Review the size and mix of the ODNI workforce—to include the ratio between cadre and detailees, the balance between government and contractors, and grade structure—to perform its roles, missions and functions; and
- (8) Make recommendations regarding the above.

The Agreement directs the President, no later than 30 days after the enactment of this Act, to select the individuals who will serve on the external panel and notify the congressional intelligence committees of such selection.

In addition, the Agreement directs the panel, no later than 180 days after the enactment of this Act, to provide a report on this review to the congressional intelligence committees. This report shall be unclassified, but may contain a classified annex. The Agreement further directs ODNI to reimburse the Executive Office of the President for any costs associated with the review.

Improving pre-publication review

The congressional intelligence committees are concerned that current and former IC personnel have published written material without completing mandatory pre-publication review procedures or have rejected changes required by the review process, resulting in the publication of classified information. The committees are particularly troubled by press reports suggesting that officials are unaware of the existence or scope of pre-publication review requirements.

The committees are also aware of the perception that the pre-publication review process can be unfair, untimely, and unduly onerous—and that these burdens may be at least partially responsible for some individuals “opting out” of the mandatory review process. The committees further understand that IC agencies’ pre-publication review mechanisms vary, and that there is no binding, IC-wide guidance on the subject.

The committees believe that all IC personnel must be made aware of pre-publication review requirements and that the review process must yield timely, reasoned, and impartial

decisions that are subject to appeal. The committees also believe that efficiencies can be identified by limiting the information subject to pre-publication review, to the fullest extent possible, to only those materials that might reasonably contain or be derived from classified information obtained during the course of an individual's association with the IC. In short, the pre-publication review process should be improved to better incentivize compliance and to ensure that personnel fulfill their commitments.

Therefore, the Agreement directs that, no later than 180 days after the enactment of this Act, the DNI shall issue an IC-wide policy regarding pre-publication review. The DNI shall transmit this policy to the congressional intelligence committees concurrently with its issuance. The policy should require each IC agency to develop and maintain a pre-publication policy that contains, at a minimum, the following elements:

- (1) Identification of the individuals subject to pre-publication review requirements ("covered individuals");
- (2) Guidance on the types of information that must be submitted for pre-publication review, including works (a) unrelated to an individual's IC employment; or (b) published in cooperation with a third party, e.g.—
 - (a) Authored jointly by covered individuals and third parties;
 - (b) Authored by covered individuals but published under the name of a third party; or
 - (c) Authored by a third party but with substantial input from covered individuals.
- (3) Guidance on a process by which covered individuals can participate in pre-publication reviews, and communicate openly and frequently with reviewers;
- (4) Requirements for timely responses, as well as reasoned edits and decisions by reviewers;
- (5) Requirements for a prompt and transparent appeal process;
- (6) Guidelines for the assertion of interagency equities in pre-publication review;
- (7) A summary of the lawful measures each agency may take to enforce its policy, to include civil and criminal referrals; and
- (8) A description of procedures for post-publication review of documents that are alleged or determined to reveal classified information but were not submitted for pre-publication review.

Additionally, the Agreement directs ODNI, no later than 180 days after the enactment of this Act, to provide to the congressional intelligence committees a report on the adequacy of IC

information technology efforts to improve and expedite pre-publication review processes, and the resources needed to ensure that IC elements can meet this direction.

The Agreement further directs the DNI, no later than 270 days after the enactment of this Act, to certify to the congressional intelligence committees that IC elements' pre-publication review policies, non-disclosure agreements, and any other agreements imposing pre-publication review obligations reflect the policy described above.

Student loan debt report

IC components need to be able to recruit talented young professionals. However, the soaring cost of college and post-graduate education in the United States is causing many young people to forgo public service in favor of career opportunities with more competitive pay or loan forgiveness benefits.

Therefore, the Agreement directs ODNI, no later than 180 days after the enactment of this Act, to provide a report to the congressional intelligence committees on programs that seek to help IC personnel manage student loan debt. The report shall include details about each IC element's program, including loan forgiveness, loan repayment, and financial counseling programs; efforts to inform prospective and current employees about such programs; and the number of employees who use such programs. The report shall also include an analysis of the benefits and drawbacks of creating new programs and expanding existing programs, and shall identify any barriers to the establishment of IC-wide programs.

Workforce development partnership

The congressional intelligence committees have long promoted novel recruiting, hiring, and retention practices, especially with respect to highly expert, highly sought-after Science, Technology, Engineering, and Math (STEM) students and professionals. Despite these efforts, the IC continues to struggle with meeting STEM recruitment, hiring, and retention goals inside the IC.

The committees are therefore encouraged to learn that the IC is considering new and creative practices in this regard. For example, the committees were intrigued by the Pacific Northwest National Laboratory's (PNNL) budding Workforce Development Partnership with the CIA. Partnerships like this may allow IC agencies to leverage PNNL's robust employee recruiting network and seek out STEM students who might not otherwise consider IC employment.

Similarly, to address concerns that potential hires will accept other job offers while awaiting clearances, NGA has a program to allow interim hires to work on unclassified projects until clearances are adjudicated. In addition, several IC agencies have instituted a unique pay scale for their junior STEM workforce. The committees recognize the benefits of these initiatives, and believes that such efforts could have wider applicability across the IC.

Therefore, the Agreement directs the DNI Chief Human Capital Officer, no later than 180 days after the enactment of this Act, to provide to the congressional intelligence committees an interagency briefing on new approaches, including outreach and advertising, the IC is considering or conducting to attract a diverse, robust Science, Technology, Engineering, and Math and information technology workforce to meet the increasing demands in the IC.

Distributed Common Ground/Surface System-Army

The congressional intelligence committees believe the Distributed Common Ground/Surface System-Army (DCGS-A) provides operational and tactical commanders with enhanced, state-of-the-art intelligence, surveillance, and reconnaissance (ISR) tasking, processing, exploitation, and dissemination capabilities and connectivity to the defense intelligence information enterprise. DCGS-A is a critical tool for enabling military intelligence warfighters to process, fuse, and exploit data. In the past, the Army has struggled to keep pace for pre-deployment and in-theater training for DCGS-A. However, training for military intelligence analysts must be prioritized in the pre-deployment readiness cycle to ensure that those using this intelligence tool can effectively utilize its capabilities.

The Army has fielded over 95 percent of DCGS-A Increment 1 systems, with mixed results and often negative feedback from the users. The Army is in the process of fielding Increment 1, Release 2, which will address many of the initial concerns and deficiencies of Increment 1. The committees remain concerned that the Army has not sufficiently planned for user training in support of the release of Increment 1, Release 2 to operational users.

Therefore, the congressional intelligence committees request that the Army, no later than 90 days after the enactment of this Act, submit a plan to the congressional intelligence and defense committees on how the Army will fully incorporate Distributed Common Ground/Surface System-Army (DCGS-A) training into the readiness cycle for Army personnel. The plan should specifically address any lessons learned from the fielding of DCGS-A Increment 1 and any ongoing corrective actions to improve the roll-out of Increment 1, Release 2.

Common controller for unmanned aircraft systems

The congressional intelligence committees support the Army's efforts to develop a common controller for the RQ-7A/B Shadow and the RQ-11B Raven tactical unmanned aerial vehicles. However, the committees are concerned that the Army is not collaborating with the Marine Corps on similar efforts to develop a ground controller for the Marine Corps family of tactical unmanned aerial systems (UAS), including the RQ-11B Raven, the RQ-12A Wasp, and the RQ-20A Puma.

Therefore, the Agreement requests that the Army and the Marine Corps Intelligence Activity (MCIA), no later than 90 days after the enactment of this Act, jointly submit a report to the congressional intelligence and defense committees on the feasibility of developing a common controller for all Brigade and Below unmanned aircraft systems (UAS) airframes, as well as U.S. Marine Corps small unit UAS. The report should address the potential performance and operational benefits of a common controller, anticipated development costs, and anticipated life-cycle cost savings of a common controller.

Review of dual-hatting relationship

The congressional intelligence committees support further evaluation of the dual-hatting of a single individual as both Commander of U.S. Cyber Command (USCYBERCOM) and Director of the National Security Agency (DIRNSA).

Therefore, the Agreement directs the Secretary of Defense, no later than 90 days after the enactment of this Act, to provide to the congressional intelligence and defense committees a briefing that reviews and provides an assessment of the dual-hatting of DIRNSA and Commander, USCYBERCOM. This briefing should address:

- (1) Roles and responsibilities, including intelligence authorities, of USCYBERCOM and NSA;
- (2) Assessment of the current impact of the dual-hatting relationship, including advantages and disadvantages;
- (3) Plans and recommendations on courses of action that would be necessary to end the dual-hatting of DIRNSA and Commander, USCYBERCOM, which satisfy Section 1642 of the conference report accompanying S. 2943, the National Defense Authorization Act for Fiscal Year 2017;
- (4) Suggested timelines for carrying out such courses of action;
- (5) Recommendations for any changes in law that would be required by the end of dual-hatting; and
- (6) Any additional topics as identified by the intelligence and defense committees.

The congressional intelligence committees further believe that a larger organizational review of NSA should be conducted with respect to the eventual termination of the dual-hatting relationship. The congressional intelligence committees seek to promote the efficient and effective execution of NSA's national intelligence mission. Specifically, the congressional intelligence committees believe that the organization of NSA should be examined to account for the evolution of its mission since its establishment, the current structure of the intelligence community, and the fact that the NSA is predominantly funded through the NIP.

Therefore, the Agreement further directs the DNI, no later than 120 days after the enactment of this Act, to conduct an assessment and provide a briefing to the congressional intelligence committees on options to better align the structure, budgetary procedures, and oversight of NSA with its national intelligence mission in the event of a termination of the dual-hatting relationship. This briefing should include:

- (1) An assessment of the feasibility of transitioning NSA to civilian leadership appointed by the DNI in lieu of military leadership appointed by the Secretary of Defense;

(2) How NSA could be organizationally separated from DoD if USCYBERCOM were elevated to become a unified combatant command; and

(3) Any challenges, such as those requiring changes in law, associated with such a separation.

Acquisition security improvement

The congressional intelligence committees remain concerned about supply chain and cybersecurity vulnerabilities in the IC. The committees believe the IC should implement a more comprehensive approach to address these vulnerabilities, particularly during the acquisition process. However, ICD 801, the IC guideline governing the acquisition process, is outdated and must be revised to reflect current risks. In particular, despite issuance of ICD 731, *Supply Chain Risk Management*, in 2013, ICD 801 has not been updated to reflect this policy nor does it include consideration of cybersecurity vulnerabilities and mitigation.

Therefore, the Agreement directs ODNI, no later than 180 days after the enactment of this Act, to review and consider amendments to Intelligence Community Directive (ICD) 801 to better reflect and anticipate supply chain and cybersecurity risks and threats, as well as to outline policies to mitigate both risks and threats. In particular, the review should examine whether to:

- (1) Expand risk management criteria in the acquisition process to include cyber and supply chain threats;
- (2) Require counterintelligence and security assessments as part of the acquisition and procurement process;
- (3) Propose and adopt new education requirements for acquisition professionals on cyber and supply chain threats; and
- (4) Factor in the cost of cyber and supply chain security.

The Agreement further directs ODNI, no later than 210 days after the enactment of this Act, to provide to the congressional intelligence committees a report describing the review, including ODNI's process for considering amendments to ICD 801, and specifically addressing ODNI's analysis and conclusions with respect to paragraphs (1) through (4) above.

Cyber information sharing and customer feedback

The congressional intelligence committees commend NSA's new policies and procedures to facilitate greater information sharing of cyber threat indicators and defensive measures with the Department of Homeland Security (DHS) at the unclassified level.

With the recent enactment of the Cybersecurity Act of 2015, which encourages greater information sharing between private sector stakeholders, as well as with government entities, the committees believe the next step is to ensure the entire IC is working to disseminate timely,

actionable information to private sector stakeholders so they can better protect their information technology networks. The vast majority of U.S. networks reside in the private sector, and it is good governance to ensure that those networks are safe and secure for the general public.

The committees appreciate that the IC has begun efforts to increase unclassified cyber threat sharing. Because an increase in the quantity of reporting does not necessarily indicate effectiveness or usefulness, this Committee continues to monitor the quality of the information distributed.

Therefore, the Agreement directs ODNI, no later than 120 days after the enactment of this Act, to brief the congressional intelligence committees on IC-wide efforts to share more information with the Department of Homeland Security (DHS) for further dissemination to the private sector. This briefing shall specifically address types of information shared, metrics on output, tabulation of low output producing agencies, recommendations on how low output agencies can increase sharing, timeliness of information shared, and average total time it takes for information to transit the system.

The Agreement also directs ODNI, in coordination with the DHS Office of Intelligence and Analysis (I&A), to conduct a survey of government and private sector participants of the National Cybersecurity and Communications Integration Center (NCCIC). The survey shall be anonymous, provide an accurate assessment of the usefulness and timeliness of the data received, and determine if customers are satisfied with intelligence briefings on threat actors impacting their specific industry. The Agreement further directs ODNI, no later than one year after the enactment of this Act, to provide to the congressional intelligence and homeland security committees an unclassified report detailing the results of this survey.

Department of Homeland Security utilization of National Labs expertise

The congressional intelligence committees believe that the Department of Energy (DOE) National Labs represent a unique and invaluable resource for the government and the IC in particular.

Therefore, the Agreement directs, no later than 180 days after the enactment of this Act, DHS I&A, in coordination with DOE Office of Intelligence and Counterintelligence (DOE-IN), to provide to the congressional intelligence committees a report on the current utilization of Department of Energy (DOE) National Labs expertise by DHS I&A. This report should address opportunities to increase DHS I&A's utilization of cybersecurity expertise of the National Labs as well as the budgetary implications of taking advantage of these potential opportunities.

Cybersecurity courses for Centers of Academic Excellence

The congressional intelligence committees are concerned by a recent analysis from a security firm, which determined that not one of the nation's leading undergraduate computer science programs requires students to take a cybersecurity course before graduating. Cybersecurity depends on IC professionals having a strong understanding of the cyber threat and how to mitigate it—which in turn requires a strong academic background. NSA and DHS co-sponsor the Centers of Academic Excellence (CAE) in Cyber Defense program, which includes

an emphasis on basic cybersecurity. Nevertheless, even some CAE-designated institutions lack cybersecurity course prerequisites in their computer science curricula.

Therefore, the Agreement directs ODNI, no later than 180 days after the enactment of this Act, to submit to the congressional intelligence committees a report on improving cybersecurity training within NIP-funded undergraduate and graduate computer science programs. The report should specifically address:

- (1) The potential advantages and disadvantages of conditioning an institution's receipt of such funds on its computer science program's requiring cybersecurity as a precondition to graduation;
- (2) How Centers of Academic Excellence programs might bolster cybersecurity educational requirements; and
- (3) Recommendations to support the goal of ensuring that federally-funded computer science programs properly equip students to confront future cybersecurity challenges.

PART III: SECTION-BY-SECTION ANALYSIS AND EXPLANATION OF LEGISLATIVE TEXT

The following is a section-by-section analysis and explanation of the Intelligence Authorization Act for Fiscal Year 2017.

TITLE I—INTELLIGENCE ACTIVITIES

Section 101. Authorization of appropriations

Section 101 lists the United States Government departments, agencies, and other elements for which the Act authorizes appropriations for intelligence and intelligence-related activities for Fiscal Year 2017.

Section 102. Classified Schedule of Authorizations

Section 102 provides that the details of the amounts authorized to be appropriated for intelligence and intelligence-related activities and the applicable personnel levels by program for Fiscal Year 2017 are contained in the classified Schedule of Authorizations and that the classified Schedule of Authorizations shall be made available to the Committees on Appropriations of the Senate and House of Representatives and to the President.

Section 103. Personnel ceiling adjustments

Section 103 provides that the DNI may authorize employment of civilian personnel in Fiscal Year 2017 in excess of the number of authorized positions by an amount not exceeding three percent of the total limit applicable to each IC element under Section 102, and ten percent of the number of civilian personnel authorized under such schedule for the purposes of contractor

conversions. The DNI may do so only if necessary to the performance of important intelligence functions.

Section 104. Intelligence Community Management Account

Section 104 authorizes appropriations for the Intelligence Community Management Account (ICMA) of the DNI and sets the authorized personnel levels for the elements within the ICMA for Fiscal Year 2017.

TITLE II—CENTRAL INTELLIGENCE AGENCY RETIREMENT AND DISABILITY SYSTEM

Section 201. Authorization of appropriations

Section 201 authorizes appropriations in the amount of \$514,000,000 for Fiscal Year 2017 for the Central Intelligence Agency Retirement and Disability Fund.

TITLE III—GENERAL INTELLIGENCE COMMUNITY MATTERS

Section 301. Restriction on conduct of intelligence activities.

Section 301 provides that the authorization of appropriations by the Act shall not be deemed to constitute authority for the conduct of any intelligence activity that is not otherwise authorized by the Constitution or laws of the United States.

Section 302. Increase in employee compensation and benefits authorized by law.

Section 302 provides that funds authorized to be appropriated by the Act for salary, pay, retirement, and other benefits for federal employees may be increased by such additional or supplemental amounts as may be necessary for increases in compensation or benefits authorized by law.

Section 303. Support to nonprofit organizations assisting intelligence community employees.

Section 303 permits the DNI to engage in fundraising in an official capacity for the benefit of nonprofit organizations that provide support to surviving family members of a deceased employee of an element of the IC or otherwise provide support for the welfare, education, or recreation of IC employees, former employees, or their family members. Section 303 requires the DNI to issue regulations ensuring that the fundraising authority is exercised consistent with all relevant ethical limitations and principles. Section 303 further requires that the DNI and the Director of the CIA notify the congressional intelligence committees within seven days after they engage in such fundraising.

Section 304. Promotion of science, technology, engineering, and mathematics education in the intelligence community.

Section 304 requires the DNI to submit a five-year investment strategy for outreach and recruiting efforts in the fields of science, technology, engineering, and mathematics (STEM), to include cybersecurity and computer literacy. Section 304 further requires elements of the IC to submit STEM investment plans supporting this strategy for each of the fiscal years 2018 through 2022, along with the materials justifying the budget request of each element for these STEM recruiting and outreach activities.

Section 305. Retention of employees of the intelligence community who have science, technology, engineering, or mathematics expertise.

Section 305 authorizes a new payscale to permit salary increases for employees in the IC with STEM backgrounds. Section 305 also requires notifications to individual employees if a position is removed from this new payscale. Section 305 further requires the head of each IC element to submit to the congressional intelligence committees a report on the new rates of pay and number of positions authorized under this payscale.

Section 306. Management of intelligence community personnel

Section 306 prohibits the Congress's use of government personnel ceilings in the management of the IC workforce starting in Fiscal Year 2019. Section 306 requires the DNI to provide briefings on the IC's initiative to maintain both employees and contractors within the IC, as well as both a briefing and a report on the methodology, cost analysis tool, and implementation plans. Section 306 further requires the IC IG to provide a written report on the accuracy of IC workforce data. This section will align the IC's management of personnel consistent with the practices of the Department of Defense and other federal agencies.

Section 307. Modifications to certain requirements for construction of facilities

Section 307 clarifies that the requirement to notify the congressional intelligence committees of improvement projects with an estimated cost greater than \$1,000,000 for facilities used primarily by IC personnel includes repairs and modifications.

Section 308. Guidance and reporting requirement regarding interactions between the intelligence community and entertainment industry.

Section 308 requires the DNI to issue public guidance regarding engagements by elements of the Intelligence Community with entertainment industry entities. The guidance will include DNI providing an annual report to the congressional intelligence committees detailing interactions between the IC and the entertainment industry. Section 308 also requires the report to include a description of the nature, duration, costs, benefits, and results of each engagement, as well as a determination that each engagement did not result in a disclosure of classified information and whether any information was declassified for the disclosure. Section 308 further requires that before an IC element may engage with the entertainment industry, the head of that

element must approve the proposed engagement. Contractual relationships for professional services and technical expertise are exempt from these reporting requirements.

Section 309. Protections for independent inspectors general of elements of the intelligence community.

Section 309 requires the ODNI to develop and implement a uniform policy for each identified Inspector General (IG) office in the IC to better ensure their independence. The provision specifies elements to be incorporated in such a policy including (a) guidance regarding conflicts of interest, (b) standards to ensure independence, and (c) a waiver provision. Section 309 further prohibits the DNI from requiring an employee of an OIG to rotate to a position in the element for which such office conducts oversight.

Section 310. Congressional oversight of policy directives and guidance.

Section 310 requires the DNI to submit to the congressional intelligence committees notifications and copies of any classified or unclassified Presidential Policy Directive, Presidential Policy Guidance, or other similar policy document issued by the President which assigns tasks, roles, or responsibilities to the IC, within the specified timeframes. Section 310 further requires the Director to notify the congressional intelligence committees of guidance to implement such policies.

Section 311. Notification of memoranda of understanding.

Section 311 requires the head of each element of the IC to submit to the congressional intelligence committees copies of each memorandum of understanding or other agreement regarding significant operational activities or policy entered into between or among such element and any other entity or entities of the federal government within specified timeframes.

Section 311 does not require an IC element to submit to the congressional intelligence committees any memorandum or agreement that is solely administrative in nature, including a memorandum or agreement regarding joint duty or other routine personnel assignments. An IC element also may redact any personally identifiable information from a memorandum or agreement which must be submitted to the intelligence committees.

Section 312. Technical correction to Executive Schedule

Section 312 contains a technical correction regarding the annual rate of basic pay for the Director of the National Counter Proliferation Center.

Section 313. Maximum amount charged for declassification reviews

Section 313 prohibits the head of an element of the IC from charging reproduction fees for a mandatory declassification review in excess of reproduction fees that the head would charge for a request for information under the Freedom of Information Act (FOIA). It also

permits agency heads to waive processing fees for declassification reviews in the same manner as for FOIA.

TITLE IV—MATTERS RELATING TO ELEMENTS OF THE INTELLIGENCE COMMUNITY

SUBTITLE A—OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Section 401. Designation of the Director of the National Counterintelligence and Security Center.

Section 401 renames the National Counterintelligence Executive as the “National Counterintelligence and Security Center,” with conforming amendments.

Section 402. Analyses and impact statements by Director of National Intelligence regarding proposed investment into the United States.

Section 402 directs the DNI to submit to the congressional intelligence committees, after the completion of a review or an investigation of any proposed investment into the United States, any analytic materials prepared by the DNI. This requirement includes, but is not limited to, national security threat assessments provided to the Committee on Foreign Investment in the United States (CFIUS) in connection with national security reviews and investigations conducted by CFIUS pursuant to Section 721(b) of the Defense Production Act of 1950 (50 U.S.C. § 4565). This section is not intended to limit the ability of the DNI to transmit supplementary materials to the congressional intelligence committees along with the threat assessments.

Section 402 also directs the DNI to provide the committees with impact statements when the DNI determines a proposed investment into the United States will have an operational impact on the IC.

Section 403. Assistance for governmental entities and private entities in recognizing online violent extremist content

Section 403 requires the DNI to publish on a publicly available Internet website a list of all logos, symbols, insignia, and other markings commonly associated with, or adopted by, State Department-designated foreign terrorist organizations.

SUBTITLE B—CENTRAL INTELLIGENCE AGENCY

Section 411. Enhanced death benefits for personnel of the Central Intelligence Agency.

Section 411 authorizes the Director of the CIA to pay death benefits substantially similar to those authorized for members of the Foreign Service, and requires the Director to submit implementing regulations to the congressional intelligence committees.

Section 412. Pay and retirement authorities of the Inspector General of the Central Intelligence Agency.

Section 412 amends the Central Intelligence Agency Act of 1949 to authorize the IG of the CIA to consider certain positions as law enforcement officers for purposes of calculating retirement eligibility and entitlements under chapters 83 and 84 of title 5, United States Code, if such officer or employee is appointed to a position with responsibility for investigating suspected offenses against the criminal laws of the United States. Section 412 may not be construed to confer on the IG of the CIA, or any other officer or employee of the CIA, any police or law enforcement or internal security functions or authorities.

SUBTITLE C—OTHER ELEMENTS

Section 421. Enhancing the technical workforce for the Federal Bureau of Investigation.

Section 421 requires the Federal Bureau of Investigation (FBI) to produce a comprehensive strategic workforce report to demonstrate progress in expanding initiatives to effectively integrate information technology expertise in the investigative process. Section 421 further requires the report to include: (1) progress on training, recruitment, and retention of cyber-related personnel; (2) an assessment of whether FBI officers with these skill sets are fully integrated in the FBI's workforce; (3) the FBI's collaboration with the private sector on cyber issues; and (4) an assessment of the utility of reinstituting and leveraging the FBI Director's Advisory Board.

Section 422. Plan on assumption of certain weather missions by the National Reconnaissance Office

Section 422 requires the Director of the NRO to develop a plan to carry out certain space-based environmental monitoring missions currently performed by the Air Force. It also authorizes certain pre-acquisition activities and directs that an independent cost estimate be submitted to the congressional intelligence and defense committees. The Director of NRO may waive the requirement of Section 422 if the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Chairman of the Joint Chiefs of Staff, jointly submit a certification to the congressional intelligence and defense committees.

TITLE V—MATTERS RELATING TO FOREIGN COUNTRIES

Section 501. Committee to counter active measures by the Russian Federation to exert covert influence over peoples and governments.

Nothing in this section shall authorize the Committee to take action with regard to activities protected by the First Amendment. Section 501 requires the President to establish an interagency committee to counter active measures by the Russian Federation that constitute Russian actions to exert covert influence over peoples and governments.

Section 502. Limitation on travel of accredited diplomats of the Russian Federation in the United States from their diplomatic post.

Section 502 requires the Secretary of State, in coordination with the Director of the FBI and the DNI, to establish an advance notification regime governing all Russian Federation accredited diplomatic and consular personnel in the United States, as well as to take action to secure compliance and address noncompliance with the notification requirement. Section 502 also requires the Secretary of State, the Director of the FBI, and the DNI to develop written mechanisms to share such travel information and address noncompliance. Section 502 further requires written reporting to the specified committees detailing the number of notifications, and the number of known or suspected violations of such personnel requirements.

Section 503. Study and report on enhanced intelligence and information sharing with Open Skies Treaty member states.

Section 503 requires the DNI, with support of other federal agencies, to conduct a study to determine the feasibility of creating an intelligence sharing arrangement and database among parties to the Open Skies Treaty (OST) with higher frequency, quality, and efficiency than that currently provided by the parameters of the OST. Section 503 also requires the Director to issue a report that includes an intelligence assessment on Russian Federation warfighting doctrine, the extent to which Russian Federation flights under the Open Skies Treaty contribute to the warfighting doctrine, a counterintelligence analysis as to the Russian Federation's capabilities, and a list of the covered parties that have been updated with this information.

TITLE VI—REPORTS AND OTHER MATTERS

Section 601. Declassification review of information on Guantanamo detainees and mitigation measures taken to monitor the individuals and prevent future attacks.

Section 601 requires the DNI to complete a declassification review of intelligence reports prepared by the National Counterterrorism Center (NCTC) on the past terrorist activities of each Guantanamo detainee, for a detainee's Periodic Review Board (PRB) sessions, transfer, or release from Guantanamo. To the extent a transfer or release preceded the PRB's establishment, or the NCTC's preparation of intelligence reports, Section 601 requires the DNI to conduct a declassification review of intelligence reports containing the same or similar information as the intelligence reports prepared by the NCTC for PRB sessions, transfers, or releases.

Section 601 further requires the President to make any declassified intelligence reports publicly available, including unclassified summaries of measures being taken by the transferee countries to monitor the individual and prevent future terrorist activities. Section 601 requires the DNI to submit to the congressional intelligence committees a report setting forth the results of the declassification review, including a description of covered reports that were not declassified. Section 601 also sets the schedule for such reviews and further defines past terrorist activities to include terrorist organization affiliations, terrorist training, role in terrorist attacks, responsibility for the death of United States citizens or members of the Armed Forces, any admission thereof, and a description of the intelligence supporting the past terrorist activities, including corroboration, confidence level, and any dissent or reassessment by the IC.

Section 602. Cyber Center for Education and Innovation Home of the National Cryptologic Museum.

Section 602 amends 10 U.S.C. § 449 to enable the establishment of a Cyber Center for Education and Innovation-Home of the National Cryptologic Museum (the "Center"). Section 602 also establishes in the Treasury a fund for the benefit and operation of the Center.

Section 603. Report on national security systems.

Section 603 requires the Director of the National Security Agency, in coordination with the Secretary of Defense and Chairman of the Joint Chiefs of Staff to submit to the appropriate congressional committees a report on national security systems.

Section 604. Joint facilities certification.

Section 604 requires that before an element of the IC purchases, leases, or constructs a new facility that is 20,000 square feet or larger, the head of that element must first certify that all prospective joint facilities have been considered, that it is unable to identify a joint facility that meets its operational requirements, and it must list the reasons for not participating in joint facilities in that instance.

Section 605. Leadership and management of space activities.

Section 605 requires the DNI, in consultation with the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, to issue an update to the strategy for a comprehensive review of the United States national security overhead satellite architecture required in the Intelligence Authorization Act for Fiscal Year 2016. Section 605 requires the DNI, in consultation with the Secretary of Defense, to submit a plan to functionally integrate the IC's governance, operations, analysis, collection, policy, and acquisition activities related to space and counterspace. The congressional intelligence committees believe the current fragmented arrangement across the IC does not provide sufficient coherence to meet the threat, fosters duplication, hinders integrated congressional oversight, and impedes effective alignment with the Department of Defense space activities. Section 605 also requires the DNI to submit a workforce plan for space and counterspace operations, policy, and acquisition. Section 605 further requires the Director of the NRO and the Commander of U.S. Strategic Command to

submit a concept of operations and requirements documents for the Joint Interagency Combined Space Operations Center, and to conduct quarterly update briefings.

Section 606. Advances in life sciences and biotechnology.

The congressional intelligence committees recognize the rapid advancements in the life sciences and biotechnology and firmly believes that biology in the twenty-first century will transform the world as physics did in the twentieth century. The potential risks associated with these advancements are less clear. The posture of the IC to follow and predict this rapidly changing landscape is a matter of concern recognizing the global diffusion and dual-use nature of life sciences and biotechnology along with the dispersed responsibility of the life sciences related issues across several National Intelligence Officer portfolios.

Section 606 requires the DNI to brief the congressional intelligence committees and the congressional defense committees on a proposed plan and actions to monitor advances in life sciences and biotechnology to be carried out by the DNI. The Director's plan should include, first, a description of the IC's approach to leverage the organic life science and biotechnology expertise both within and outside the Intelligence Community; second, an assessment of the current life sciences and biotechnology portfolio, the risks of genetic editing technologies, and the implications of these advances on future biodefense requirements; and, third, an analysis of organizational requirements and responsibilities to include potentially creating new positions. Section 606 further requires the DNI to submit a written report and provide a briefing to the congressional intelligence committees and the congressional defense committees on the role of the IC in the event of a biological attack, including a technical capabilities assessment to address potential unknown pathogens.

Section 607. Reports on declassification proposals.

Section 607 requires the DNI to provide the congressional intelligence committees with a report and briefing on the IC's progress in producing four feasibility studies undertaken in the course of the IC's fundamental classification guidance review, as required under Executive Order 13526. Section 607 further requires the Director to provide the congressional intelligence committees with a briefing, interim report, and final report on the final feasibility studies produced by elements of the IC and an implementation plan for each initiative.

Section 608. Improvement in government classification and declassification.

Section 608 assesses government classification and declassification in a digital era by requiring the DNI to review the system by which the Government classifies and declassifies national security information to improve the protection of such information, enable information sharing with allies and partners, and support appropriate declassification. Section 608 requires the DNI to submit a report with its findings and recommendations to the congressional intelligence committees. Section 608 further requires the DNI to provide an annual written notification to the congressional intelligence committees on the creation, validation, or substantial modification (to include termination) of existing and proposed controlled access programs, and the compartments and subcompartments within each. This certification shall

include the rationale for each controlled access program, compartment, or subcompartment and how each controlled access program is being protected.

Section 609. Report on implementation of research and development recommendations.

Section 609 requires the DNI to conduct and provide to the congressional intelligence committees a current assessment of the IC's implementation of the recommendations issued in 2013 by the National Commission for the Review of the Research and Development (R&D) Programs of the IC.

Section 610. Report on Intelligence Community Research and Development Corps.

Section 610 requires the DNI to develop and brief the congressional intelligence committees on a plan, with milestones and benchmarks, to implement a R&D Reserve Corps, as recommended in 2013 by the bipartisan National Commission for the Review of the R&D Programs of the IC, including any funding and potential changes to existing authorities that may be needed to allow for the Corps' implementation.

Section 611. Report on information relating to academic programs, scholarships, fellowships, and internships sponsored, administered, or used by the intelligence community.

Section 611 requires the DNI to submit to congressional intelligence committees a report on information that the IC collects on certain academic programs, scholarships, and internships sponsored, administered, or used by the IC.

Section 612. Report on intelligence community employees detailed to National Security Council

Section 612 requires the DNI to submit to the congressional intelligence committees a classified written report listing, by year, the number of employees of an element of the IC who have been detailed to the National Security Council during each of the previous ten years.

Section 613. Intelligence community reporting to Congress on foreign fighter flows

Section 613 directs DNI to submit to the congressional intelligence committees a report on foreign fighter flows to and from terrorist safe havens abroad.

Section 614. Report on cybersecurity threats to seaports of the United States and maritime shipping

Section 614 directs the Under Secretary of Homeland Security for Intelligence and Analysis (I&A) to submit to the congressional intelligence committees a report on the cybersecurity threats to seaports of the United States and maritime shipping.

Section 615. Report on reprisals against contractors of the intelligence community

Section 615 directs the IC IG to submit to the congressional intelligence committees a report on known or claimed reprisals made against employees of contractors of elements of the IC during the preceding three-year period. Section 615 further requires the report to include an evaluation of the usefulness of establishing a prohibition on reprisals as a means of encouraging IC contractors to make protected disclosures, and any recommendations the IC IG deems appropriate.

IC Prepublication Terms of Reference for Referrals

I. (U) REFERENCES AND AUTHORITIES:

- A. The National Security Act of 1947, as amended
- B. 50 USC 3024
- C. 50 USC 424
- D. National Security Agency Act of 1959, as amended
- E. CIA Act of 1949, as amended
- F. Executive Order 12333, as amended
- G. Executive Order 13526

II. (U) PURPOSE

The purpose of this agreement is to establish a cooperative relationship among parties to work together for the referral of agency equity discovered during pre-publication review of submissions intended for public use. This agreement describes the scope of collaboration, mutual responsibilities and agreed-upon processes to be followed for the referral of another agency's equities as part of pre-publication review. This Agreement does not supersede agreements between agencies, current or future authorities granted to agencies and elements of the Intelligence Community (IC).

III. (U) BACKGROUND

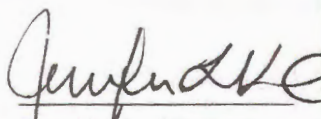
Agencies frequently receive pre-publication review submissions for public use that contain the equities of more than one agency. While informal and undocumented processes have been used to govern the protection of other agency equities, a consensus has emerged over time that recognizes the need to formalize and standardize the pre-publication referral process.

IV. (U) IMPLEMENTATION AND RESPONSIBILITIES

- A. All agencies agree to cooperate in protecting the equities of other agencies as part of the pre-publication review process. When conducting pre-publication review, all agencies will identify and refer equities that are owned, managed or otherwise the responsibility of another IC agency. The originating agency will evaluate the equities in a submission and decide if a referral is necessary. Equities that are part of a previous official acknowledgement by the equity-holding agency may not need to be referred; however, if there is any doubt, the equities will be referred. The originating agency will not give the requestor permission to publicly use the information until a determination by the equity owner has been made. The originating agency will coordinate all input from other agencies and consolidate it into a single, comprehensive response to the requestor.

- B. When an agency receives a referral, it will strive to respond to the referring agency within the timeframe identified by the referring agency. If this timeline is not attainable because of complexity, size, or operational tempo, it will notify the originating agency as soon as possible before the deadline for a response passes.
- C. All agencies agree to provide a written acknowledgment of receipt to the originating agency within two business days upon receipt of the referral.
- D. All agencies agree to establish and identify to other agencies a single point of entry for pre-publication review referrals. In addition, all agencies agree to provide updates or changes to their pre-publication referral coordination process. Agencies should not utilize an individual POC or named individual in order to minimize disruption to the process.
- E. All agencies agree to use the Joint Worldwide Intelligence Communications System (JWICS) as the standard pre-publication referral medium. Use of JWICS will protect referrals from unauthorized disclosure when they are transmitted to equity-owning agencies, when responses are communicated by those agencies, and until the pre-publication review process is complete. If referrals must be transmitted on another network, the originating agency must ensure the level of classification is appropriate before transmitting.
- F. Agencies agree to use clear language when providing the originating agency a response. Responses should clearly indicate what equities may be used publicly, what modifications are required prior to public use, and what equities are to remain protected. It is the responsibility of the originating agency to fully understand any restrictions or redactions before a response is given to the requestor.

V. (U//FOUO) This Agreement goes into effect as of 1 September 2015 with completion of signatures below:

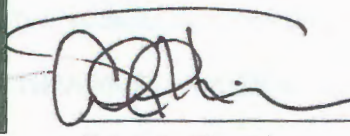


Jennifer L. Hudson
Director, IMD
ODNI

(b)(6)



Joseph W. Lambert
Director, IMS
CIA



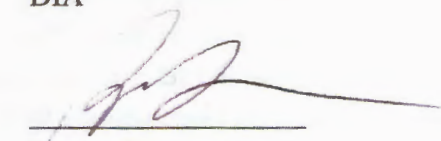
Caleb L. Temple
Director, OCC
DIA



William M. Caniano
Director, OCC
NGA



Stephen R. Glenn
Chief, IMSO
NRO



Patrick Bomgardner
Chief, ISP
NSA

UNCLASSIFIED

National Geospatial-Intelligence Agency

INSTRUCTION

NUMBER 5720.1

12 May 2015

OCC

SUBJECT: Clearance for Public Release

References: See Enclosure 1.

1. PURPOSE. This Instruction:

a. Establishes policy, assigns responsibilities, and prescribes guidance to ensure all procedures for the review of NGA information intended for public release are carried out to prevent the unintended release of classified or sensitive unclassified information.

b. Incorporates and rescinds NGA Instruction (NI) 5720.1R10, "Clearance for Public Release," 08 December 2008 (Reference (h)).

2. APPLICABILITY. This Instruction applies to NGA civilian employees, military service members, personnel from other Government agencies permanently assigned to NGA, and contractors. Exceptions are noted in Enclosure 5.

3. POLICY. It is NGA policy that:

a. Any official NGA-related information intended for public release that pertains to military or intelligence matters, national security issues, or subjects of significant concern to the Department of Defense (DoD), the US Intelligence Community, NGA, and/or its foreign and domestic partners must be reviewed prior to release;

b. The public release of official NGA-related information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate governmental interests as prescribed in References (b-f); and

c. NGA-related information intended for public release is both accurate and timely and is provided in a manner consistent with current Agency branding and messaging protocols.

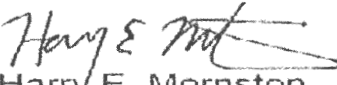
4. RESPONSIBILITIES. See Enclosure 2.**UNCLASSIFIED**

UNCLASSIFIED

NGAI 5720.1

5. PROCEDURES. See Enclosure 3.

6. EFFECTIVE DATE. This Instruction is effective on the date of signature.


Harry E. Mornston
Chief of Staff

Enclosures

1. References
2. Responsibilities
3. Procedures
4. Process Flow Diagram
5. Exceptions to the Public Release Process
6. Areas of Special Consideration
7. Markings

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 1REFERENCES

- (a) Title 10, United States Code, Section 424
- (b) DoD Directive (DoDD) 5230.9, "Clearance of DoD Information for Public Release," 22 August 2008
- (c) DoDD 5400.7, "DoD Freedom of Information Act Program," 02 January 2008
- (d) DoDD 5400.11, "DoD Privacy Program," 29 October 2014
- (e) DoD Instruction (DoDI) 5230.29, "Security and Policy Review of DoD Information for Public Release," 13 August 2014
- (f) DoDI 8550.01, "DoD Internet Services and Internet-Based Capabilities," 11 September 2012
- (g) NGA Instruction (NI) 5505.2R4, "Release of Information in Litigation and Testimony," 24 November 2003
- (h) NI 5720.1R10, "Clearance for Public Release," 08 December 2008 (hereby rescinded)
- (i) NI 5720.3R4, "Media and Public Interaction," 16 January 2008
- (j) NI 8900.4R6, "Intelligence Oversight Compliance and Awareness Program," 10 July 2010
- (k) NI 8955.5R5, "Preparing NGA Web Pages," 22 May 2009
- (l) "Defense Federal Acquisition Regulation Supplement (DFARS)," Part 252, 15 October 2014
- (m) "Standard Operating Procedures Regarding InnoVision or NGA Employee-Produced Software Submitted for Public Release Review," 28 May 2013
- (n) "Interim Guidance—Procedures for Marking US Person (USPER) Information and Domestic Imagery," 03 September 2014
- (o) Memorandum for the Director of National Intelligence, "Designation of National Geospatial-Intelligence Agency Senior Foreign Disclosure and Release Authority," 29 April 2013

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 2RESPONSIBILITIES

1. Director, Office of Corporate Communications (OCC).

a. Administers public release policy and coordinates the review of all print and electronic information regarding NGA mission and functions intended for public release, ensuring the information intended for public release is unclassified and is consistent with established policies.

b. Coordinates all NGA interaction with the media, ensuring information intended for release is unclassified and is consistent with established DoD, Office of the Director of National Intelligence, and NGA policies. OCC coordinates with these and other public affairs offices as necessary in accordance with Reference (i).

c. Manages the NGA brand, including Agency-level messaging, the "look and feel" of printed and electronic products, and is responsible for reviewing NGA products for adherence to Agency branding and messaging standards.

2. Director, Analysis.

a. Reviews public release submissions containing Analysis-related subject matter, as requested by OCC, as one of two NGA Senior Foreign Disclosure and Release Authorities (Reference (o)). Such subject matter includes or refers to analytic data, products, services, or tradecraft.

b. Develops a Standard Operating Procedure (SOP) establishing internal procedures that ensure a comprehensive review of materials submitted by OCC for evaluation and comment.

3. General Counsel.

a. Reviews all public release submissions for legal sufficiency and implications for release under the requirements of the Freedom of Information Act (FOIA) and the Privacy Act. The Office of General Counsel (OGC) reviews information related to but not limited to contract law, copyrights, trademarks, commercial licensing, intelligence oversight, ethics, and other statutory considerations governing NGA-related information.

b. Develops an SOP establishing internal procedures that ensure a comprehensive review of materials submitted by OCC for evaluation and comment.

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

4. Director, International Affairs (IA).

a. Reviews public release submissions containing IA-related subject matter, as requested by OCC, as one of two NGA Senior Foreign Disclosure and Release Authorities (Reference (o)). Reviews include submissions containing embedded geospatial products, imagery, imagery-derived products, and requests for restricted products; and situations where disclosure and release (D&R) standing authority is in question with regard to NGA products. When necessary, consults with managers of international programs to ensure that D&R decisions are consistent with the requirements of existing international agreements.

b. Develops an SOP establishing internal procedures that ensures a comprehensive review of materials submitted by OCC for evaluation and comment.

5. Director, Security and Installations.

a. Reviews public release submissions for potential Operations Security (OPSEC), counterintelligence, and classification considerations as requested by OCC.

b. Develops an SOP establishing internal procedures that ensures a comprehensive review of materials submitted by OCC for evaluation and comment.

6. Director, Office of Contract Services (OCS), or any other organization within NGA that executes formal arrangements with external activities.

a. Ensures, in accordance with the Defense Federal Acquisition Regulation Supplement (DFARS) (Reference (l)), that the security clause of any Agency agreement includes the requirement that any NGA-related information intended for public release be submitted to OCC (through the contracting officer) for review. This requirement applies to all NGA contracts, agreements, memoranda of understanding, grants and nontraditional procurements, and any similar arrangements over which NGA exercises operational control. However, review can be waived for articles resulting from routine research and development grants to a research or academic institution to advance a professional field. In such cases, OCS and other involved NGA organizations ensure this option is clear in the security clause.

b. Reviews contractor-submitted materials for technical accuracy and determines the appropriateness for public release prior to submitting the information to OCC for review.

7. All Other Components. Review selected materials for their respective areas of expertise on a case-by-case basis as deemed appropriate by OCC.

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 3PROCEDURES

1. Submitting Materials for Review.

a. A copy of the material in its final form and a signed NGA Form 5230-1, "[Request for Clearance for Public Release](#)," with blocks 1, 2, and 3 completed should be emailed via secure channels to the [OCC Public Release mailbox](#). Submissions sent via non-secure means will not be accepted by OCC. If the submitter is remotely located, s/he should transfer the material to a secure network and then forward to OCC. If there are special circumstances in regard to submitting materials, the submitter should contact OCC prior to attempting to submit materials via non-secure means.

b. Material submitted for review must be approved by the submitter's supervisor or designated approving official, as indicated on the NGA Form 5230-1 (block 3). The approving official should have the appropriate expertise and authority to certify that the information is technically accurate, does not contain classified or sensitive information, and is appropriate for public release. Submissions by NGA senior-level employees do not require secondary approval.

c. Abstracts to be published in advance of a completed paper, manuscript, or briefing must also be submitted to OCC for review with a completed NGA Form 5230-1. The approved public release of an abstract is not applicable to the final material that must be submitted separately for review. If an abstract is approved, the OCC case number assigned to the abstract should be noted on the NGA Form 5230-1 when the final material is submitted to OCC.

d. Submissions created wholly or in part from materials previously approved for public release must identify the approved portions (by providing the OCC-issued public release number) and the new material to be reviewed. Previously approved materials, such as briefing slides that have not been altered, must display the original public release number. Any substantive changes to any portion of previously approved materials that could or would cause a change in the interpretation or original meaning of the information will require review as a new submission.

e. Contractor Submissions.

(1) The approving authority for NGA contractor submissions that are not NGA-owned deliverables (e.g., marketing materials, company presentations, company press releases) is typically the NGA contracting officer (CO) or a designated contracting officer representative (COR) overseeing the performed work or contract award. The approving authority reviews the materials and certifies that the information is technically accurate, does not contain classified or sensitive information, is appropriate

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

for public release, and conforms to the contractual requirements. Once approved, the approving authority should complete NGA Form 5230-1 and transmit the information to OCC for review.

(2) Submissions created by embedded contractors that are deliverables and will be used as an NGA presentation or product do not require CO or COR approval. The government lead or supervisor may act as the approving official as appropriate.

(3) Personnel from other Federal agencies, private companies, or academic institutions exercising a non-traditional NGA contract, memorandum of understanding, grant, or any other type of formal agreement, such as an NGA University Research Initiative or a Cooperative Research and Development Activity, must submit NGA-related information intended for public release to the NGA organization with overall supervisory control of the agreement for initial review and further processing.

2. Review and Tasking.

a. Initial OCC Review and Tasking.

(1) OCC reviews submitted materials for completeness and obtains clarifications or additional information from the submitter as necessary.

(2) Upon receipt of a complete submission package, OCC will assign a unique public release case number to the request package for tracking purposes.

(3) Based on content of the material submitted, OCC will determine which NGA offices have potential interests in the subject matter and will request their review of the submission with a requested suspense date. At a minimum, all submissions will be reviewed by the OGC, the Security Education and Awareness OPSEC team and the Counterintelligence Office. OCC may coordinate submissions with other offices as necessary.

(4) OCC will provide all available background information and contact information for the submitter to the reviewing offices.

3. Reviewing Offices' Review.

a. Reviewing offices will, in accordance with their Component-specific public release SOP, review the submitted materials for all information related to the Component's area of expertise and reply to OCC on or before the requested suspense date with their consolidated recommendations and justifications for modifications or denial.

b. Reviewing offices should contact the submitter directly for clarifications relative to their particular areas of interest that may be needed to conduct a proper review. As necessary, reviewing offices should attempt to negotiate acceptable alternatives to

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

questionable information and, if applicable, highlight any discrepancies, inaccuracies, or inconsistencies with current Agency policy and recommend changes for the author's consideration. Negotiated changes should be reported in the reviewing office's final response to OCC.

c. If a reviewing office believes the submitted materials require additional review by another Component not already tasked for comment, the office should inform OCC as soon as possible and provide its rationale. Reviewing offices should not unilaterally request assistance from other Components.

d. "Non-concur" responses without justification from a reviewing office will be disregarded by OCC.

e. "Non-concur" responses from a reviewing office that are based on issues outside the purview of the reviewing office will be disregarded by OCC.

f. Reviewing offices will assign an NGA employee to either respond to or coordinate the Key Component's release recommendations as OGC has determined that a public release decision relative to NGA-owned information is an inherently governmental function. Release recommendations provided by contractor personnel should include evidence in the response that the recommendation has been authorized by a qualified government employee.

4. Final OCC Review and Release Decision.

a. OCC reviews, evaluates, and reconciles feedback from reviewing offices.

b. Based on recommendations from reviewing offices, OCC determines if the submission is:

(1) Approved for Public Release,

(2) Approved for Public Release with provisions, or

(3) Denied for Public Release.

c. After making a release determination, OCC advises the submitter of the release decision via email and provides relevant additional information as necessary regarding the submitted material. For denials, OCC provides the submitter the reason for the denial and contact information for the reviewing office(s) that objected to the information release.

d. OCC issues a unique public release number to all NGA-owned and branded items that have been approved for public release. The following disclaimer must be displayed on the approved product as evidence of authorization to release: "Approved for public release, XX-XXX" (insert public release number).

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

e. Materials approved for public release not owned by NGA or otherwise associated with an external entity (e.g., a technical paper written by an academic institution or contractor-owned product) are not required to display the disclaimer above.

5. Post-decision Actions for Submitters.

a. Upon receipt of OCC's decision of approval or approval with provisions, the submitter will make any required corrections, including application of the disclaimer, and provide a final corrected copy to OCC for record-keeping purposes.

b. For denials, the submitting office may appeal the decision and work directly with the objecting reviewing office(s) to reach a resolution. If an agreement is reached, the reviewing office(s) should advise OCC of the corrective measures and the submitter should provide a corrected copy of the materials to OCC. OCC will then issue a public release number for the approved materials.

6. Retired and Former Employees.

a. Protecting classified information is a life-long obligation and continues after departure from the Agency. NGA-related information in personal works destined for public release requires review by NGA for potential classification issues.

b. Human Development (HD) provides information about this process to departing employees as part of their check-out process. OCC provides information about this process via the NGA public Web site.

c. Retired and former employees seeking reviews may submit their materials directly to NGA via email at prepubreview@nga.mil.

7. Submissions Timelines. Materials submitted to OCC with a requested due date that is less than the allotted amount of time required are subject to denial or otherwise the releasability may be undetermined by the requested due date.

Type of Submission	Minimum Time Required for Review
Abstracts, speeches, standard length briefings, talking points, posters, brochures, technical or academic papers less than 25 pages in length, or other similarly sized, noncomplex products	7 business days
Technical and academic papers more than 25 pages but not exceeding 100 pages in length	10 business days
Briefings and presentations of new (not previously cleared) materials in excess of 25 pages in length	10 business days

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

Live computer-based demos, briefings, or videos that require desk-side reviews	5 business days after demo (arranged by the submitter)
Product reviews for open house events, such as Family Day and Bring Your Child to Work Day, that require desk-side reviews	10 business days
Papers, academic theses, and highly technical presentations more than 100 pages in length	30 business days
Presentations, briefings, papers, or other materials that include multi-agency interests requiring additional coordination with external organizations	30 business days (minimum) after submitting to external agency
Press and news releases	3 business days

UNCLASSIFIED

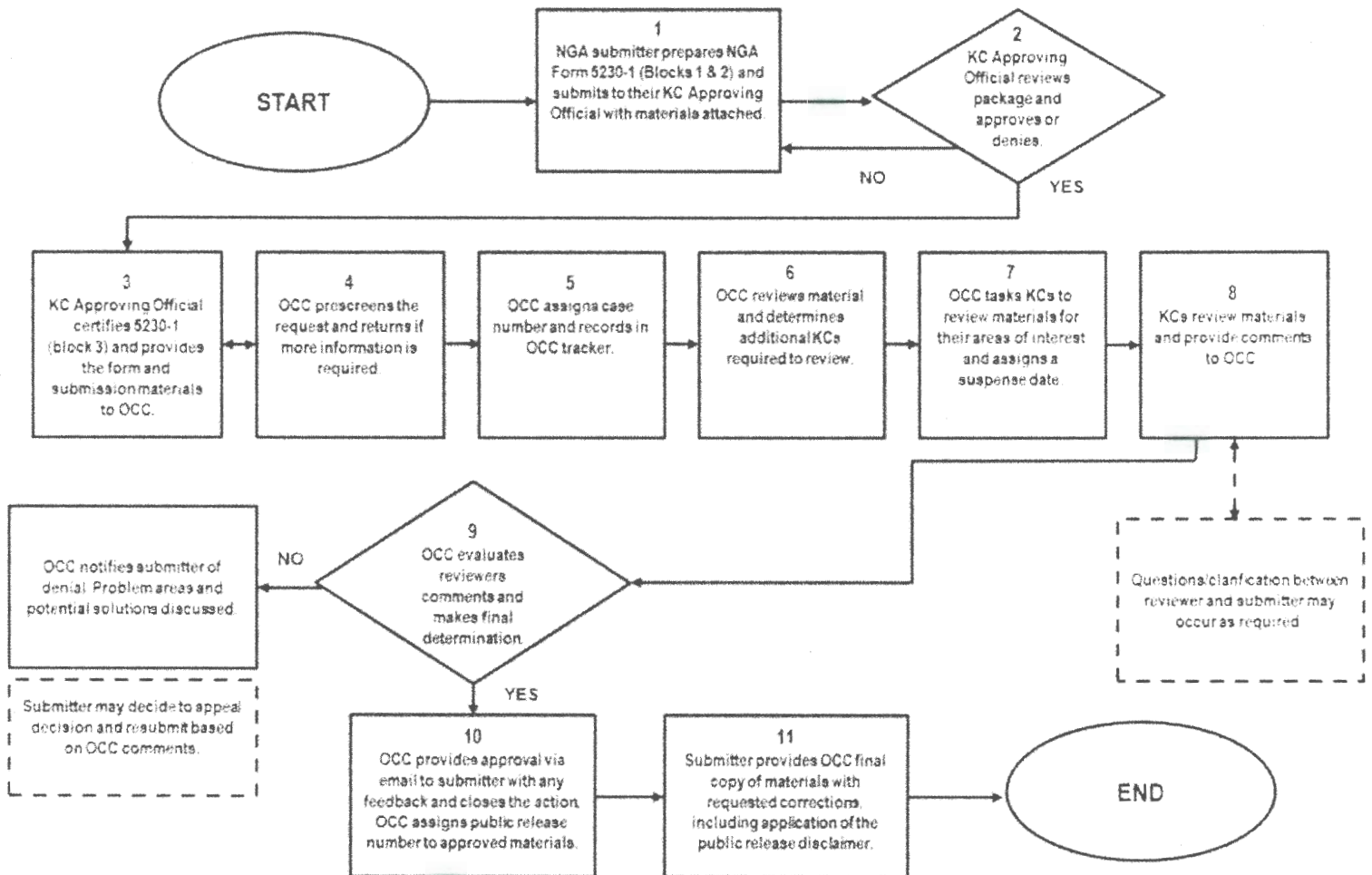
UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 4

PROCESS FLOW DIAGRAM

Clearance for Public Release Process Flow



UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 5EXCEPTIONS TO THE PUBLIC RELEASE PROCESS

The following categories of information are governed by separate review procedures and are exempted from the OCC public release review process.

1. Contract Services-generated contract-related documents or solicitations to fulfill DFARS requirements (Reference (l)) or other federally mandated requirements to publicly disseminate information regarding proposed contract actions, contract awards, and other procurement-related matters.
2. HD-generated standard job announcements posted to NGA's public-facing Web site, USAJobs, or other public venues. HD-produced materials such as brochures; flyers; videos; Web announcements for use at public events, such as job fairs and recruitment events; and other such activities are not exempt from a public release review.
3. Federally or DoD-mandated Web site notices such as the Privacy Act, FOIA, and System of Records notices.
4. Geospatial data, products, or services under the control of NGA (whether NGA or foreign-partner produced) fall under the purview of the IA's D&R branch.
5. Personal resumes requiring a classification review fall under the purview of NGA's Classification Management Office (SISCC). NGA personnel are encouraged to obtain peer and supervisor review when practicable and to use classification guides available online before contacting SISCC for assistance.
6. Products related to NGA production or developmental systems, plans, programs, or projects (e.g., technical reports, technical bulletins, product specifications) fall under the purview of the Component responsible for the effort.
7. NGA-developed software and code fall under the purview of InnoVision as stated in Reference (m).
8. All requests for release of NGA-related information or testimony to be used in legal proceedings should immediately be referred to OGC for review and guidance in accordance with Reference (g). NGA employees are prohibited from responding directly to requests to participate or support legal proceedings without first consulting with OGC.

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 6AREAS OF SPECIAL CONSIDERATION

1. Academic Works.

a. To ensure a climate of academic freedom and encourage intellectual expression, NGA students at an academy, college, university, or DoD school are not required to submit papers or materials to OCC prepared in response to academic requirements for review when they are not intended for release outside of the academic institution.

b. Academic materials intended for public release or that will be available to libraries that the public has access to must be submitted to OCC for review. Approval for public release will be granted as long as the information is unclassified (but not "official information"), does not jeopardized NGA interests, and the author accurately portrays official policy, even if the author takes issue with that policy.

c. NGA employees are reminded that all NGA-related information submitted for academic purposes to a public institution must be unclassified. If the employee has any concerns, s/he should contact SISCC for assistance.

2. Imagery.

a. Submissions that include overhead imagery must be clearly marked with the source of that imagery and applicable copyright notes must be displayed with the image.

b. Overhead imagery without an identified source will not be accepted for a public release review.

3. Domestic Imagery and US Persons (USPER) Information.

a. Due to potential intelligence oversight issues, in accordance with References (j) and (n), submissions containing domestic imagery must be accompanied by evidence of a current Proper Use Memorandum (PUM) as well as a statement certifying that the requested use is in accordance with the PUM. Additionally, submissions containing USPER information must provide evidence of a Letter of Consent (LOC) or further justification advising why an LOC is not required. Submitters should consult their Component Intelligence Oversight Officer (IOO) or OGC for assistance.

b. Submissions on behalf of external organizations (e.g., academia, private industry, nonprofits, trade organizations) that contain domestic imagery or possible USPER information should be accompanied with a description explaining whether the domestic imagery or USPER information was obtained from NGA or was directed by NGA to be

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

collected, which would require a PUM and/or LOC. Domestic imagery or USPER information collected solely at the discretion of the external organization and not held in NGA record holdings may not require a PUM or LOC. Submitters should consult their Component IOO or the OGC for assistance.

c. All domestic imagery products and products containing USPER information must be marked in accordance with Reference (n).

4. Internet Sources and Copyrighted Materials.

a. Submissions that contain information derived from the Internet, such as Google Maps™, or information that is copyrighted, must be accompanied by evidence that the authors or owners of the information have provided permission for its reuse.

b. Information regarding reuse can usually be found under "Terms of Use," "Legal," or other similar sections on the owner's Web site. Simply citing the Web address where the information is located may not be legally sufficient. Submissions containing Internet-derived or copyrighted information will not be approved for public release unless accompanied by the appropriate permissions.

5. Commercial Entities, Products, and Logos.

a. NGA materials that mention or depict commercial products, entities, or logos must display the appropriate trademark or copyright symbol.

b. NGA materials should not mention names of commercial products or entities or use commercial logos in any manner that could be interpreted as an NGA endorsement of commercial activity.

c. Additionally, NGA presentations briefed by an embedded contractor should not contain any information relative to the company affiliation of the contractor. When briefing, the contractor must ensure s/he is identified as a contractor and not as a US government employee. This can be achieved by associating her/his name or title with a contract number or by simply identifying her/himself as a contractor.

6. Nondisclosure of Personally Identifying Information (PII).

a. NGA may withhold the identity of its employees from public dissemination in accordance with statutory authority provided by Reference (a).

b. Due to OPSEC and counterintelligence concerns, NGA employee data is considered critical information, and PII data will not be exposed to the public in an effort to prevent potential targeting by foreign entities (e.g., intelligence services and terrorist groups). Of particular concern is the exposure of the identities of NGA analysts; subject-matter experts within intelligence areas of interest; NGA employees who have been

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

deployed, are likely to be eligible for deployment, or are currently deployed to locations outside the continental United States (OCONUS); and those employees who conduct OCONUS travel for official business. Case-by-case exceptions to this policy must be approved by the employee's Component approving authority listed below. Components may designate select persons from within the Component to be the spokesperson for the Component on specific topics of interest.

c. Component Spokesperson Approving Authorities.

(1) Analysis, Source, InnoVision: Director, Deputy Director, Chief of Staff, or a designee identified by the Component Director.

(2) All other Components: Director, Deputy Director, Chief of Staff, or any senior-level employee directly responsible to the spokesperson.

d. The identity of an NGA employee may not be used in a public venue without the employee's explicit permission unless her/his name has been previously approved for public release within a similar context and s/he has been specifically designated by her/his Component approving authority as an official spokesperson.

e. Employees whose jobs functionally involve routine interaction with the general public, such as recruiters, public affairs specialists, acquisition and contracting specialists, the NGA historian, the NGA Hydrographer, and others are exempt from the nondisclosure prohibition.

f. OCC reviews and approves versions of the NGA organization chart that are intended for public release. The release of the identity of NGA senior executives not depicted on the publicly available organization chart will be considered by OCC on a case-by-case basis.

g. Biographies of NGA personnel intended for public release or for use in event programs or other public venues must be reviewed and approved by OCC in accordance with this instruction. Biographies intended for public release should minimize the use of PII such as locations of residences or names of family members. Senior leader biographies prepared and posted on NGA intranets are not automatically approved for public release.

7. Media Inquiries.

a. All inquiries from the media, including radio and television stations, news and wire services, multimedia services, magazines, trade publications, Web sites, blogs, social media, and other similar organizations requesting NGA data, products, services, information or comments should be immediately referred to the NGA News and Information Services in accordance with Reference (i).

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

b. NGA employees may not provide any assistance to the media without prior authorization.

c. In situations where authorization is provided to an employee to deal directly with the media, all materials and talking points must be approved for public release in accordance with the procedures outlined in this NGAI.

8. Internet and Social Media.

a. OCC's News and Information Services manages NGA's official public Web site (www.nga.mil) and its official organizational presence on Twitter, Facebook, LinkedIn, Google+, YouTube, Spotify, and other social media platforms. OCC is responsible for the overall use, design, "look and feel," organization, and navigation of these sites. In accordance with Reference (k), OCC ensures adherence to Agency branding and messaging standards and, except as noted in Enclosure 5, is also responsible for the content and style of materials posted. NGA employees should contact OCC with requests for postings on any of these sites or to discuss new categories of postings.

b. Except as noted in Enclosure 5, new categories of information or significant updates to existing information will require review and release in accordance with the provisions of this instruction. Routine updates to existing materials are not required to be reviewed and approved.

c. Work-related comments made by NGA employees in their individual capacities on social media are generally not subject to the public release review process. Any posting or comment made by an NGA employee or contractor that could be construed as an official Agency policy or Agency position statement must be approved for public release prior to release.

d. Personnel must be aware of the exploitation of social media by NGA's adversaries and take appropriate action to preclude posting any information, sensitive or otherwise, that could provide insight into NGA's activities and operations.

9. Closed Meetings and Forums.

a. NGA personnel often participate in events that are not open to the public such as closed technical meetings and forums with other federal agencies and industry.

b. Materials created for these types of events, such as agendas and event schedules, and materials generated by event participants, such as meeting minutes and lists of action items, cannot be made available to participants or others through public venues, including public websites, unless specifically reviewed and approved for public release.

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

ENCLOSURE 7MARKINGS

1. Markings on Briefings.

a. Placement of the public release disclosure marking (see Enclosure 3, paragraph 4d). Briefing materials should have markings on the lower-left corner of all pages or slides.

b. The public release disclosure marking cannot be changed without prior approval from OCC. Information pulled from previously approved briefing materials for use in another briefing must retain the original unique public release number and be displayed on the corresponding page or slide where the information appears. Only the title page or slide and any new or changed pages or slides within the new briefing will be annotated with a new public release number. A single briefing may contain several public release numbers.

c. NGA briefings used in public forums that have been approved for public release and are marked with the public release disclosure marking should not contain any classification markings including the classification/declassification authority block, overall classification banner, and portion markings. Materials approved for public release do not need to be marked "unclassified."

d. OCC will not accept materials claimed to have been previously approved for public release unless accompanied by the previous release number. Absent the number, OCC will treat the submission as a new request and will process accordingly.

e. All NGA briefings must be prepared using the current approved template (available on OCC's Web site). Presenters preparing materials using previously approved briefings must ensure the current template is used.

f. There are rare circumstances where the National System for Geospatial Intelligence template may be used in lieu of the NGA template. These instances will be considered on a case-by-case basis.

g. The title page or slide of an NGA briefing that has been approved for public release cannot include any seal or logo other than the NGA seal that is embedded in the approved template. The use of office or program logos on the title page or slide of a NGA presentation being used in any public venue is strictly prohibited.

h. Use of office or program logos or seals may be acceptable on briefing materials that are for internal NGA use only as long as the logo is subordinate in size and placement to the NGA seal. This does not preclude the display of a seal or logo in

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

materials for illustrative or informational purposes. The OCC Outreach and Branding Division is responsible for the Agency's logos and should be consulted before submitting materials for review.

2. Other Hardcopy Materials. Placement of the public release disclosure marking on other hardcopy materials (such as posters, brochures, flyers, booklets) should be done in a manner that allows the observer to quickly determine that the information has been approved for public release.

3. Multimedia Materials. Multimedia presentations that have been approved for public release should depict the NGA public release disclosure marking at the beginning of the presentation, or for CD or DVD discs, on the face of the disk and additionally within the presentation. Actual placement of the marking will be at the discretion of the producer.

4. Modified Materials Previously Approved For Public Release.

a. Any change to materials previously approved for public release will require a new review by OCC for continued use in a public forum.

b. Materials submitted for re-review should include documentation indicating the original public release number with any changes in the material highlighted.

c. At the discretion of OCC, materials may be eligible for continued release under the original public release number (usually when the modifications are insignificant). Substantial changes, however, will be cause for a full re-examination of the materials.

5. Additional Markings. There are unique situations in which there may be a requirement to modify the standard public release disclosure marking or otherwise apply additional markings to NGA materials being utilized in public forums to meet unique mission requirements. Only OCC can authorize the use of these markings. Some examples are provided below:

a. "Products and/or services described may only be available to authorized customers." This marking may be required in addition to the standard public release disclosure marking in circumstances in which the information is clearly intended for a customer audience but the details are not inherently sensitive enough to warrant withholding from the public. The addition of this marking is intended to notify members of the general public with access to the materials that the products and services being described have restricted availability and are not available to the general public.

b. "Approved for Family Day use only" or "Approved for Bring Your Child to Work Day use only". These markings may be approved for use only at the discretion of OCC on materials that otherwise are not sensitive but may contain PII of NGA employees that would not normally be made publicly available. Use of this marking would allow the release of these types of materials only within an NGA facility to family members and

UNCLASSIFIED

UNCLASSIFIED

NGAI 5720.1

guests who have been authorized to attend the subject events. These markings would be used in lieu of the standard public release disclosure marking. Under no circumstances may any material containing restricted information, such as For Official Use Only, Limited Distribution, or Law Enforcement Sensitive, be used for such events.

UNCLASSIFIED

National Reconnaissance Office
Business Function 50, Information Technology,
Information Assurance, and Information Management
Directive 56-2, Access and Release
Instruction 56-2-2, Prepublication Review



26 FEBRUARY 2013

000075
UNCLASSIFIED

NI 56-2-2, Prepublication Review
FY 2013

TABLE OF CONTENTS

56-2-2 CHANGE LOG	3
SECTION I - INTRODUCTION.....	4
SECTION II - NBF 50 PREPUBLICATION REVIEW SUB-PROCESS DOCUMENTATION..	4
Governing NBF.....	4
Description.....	4
Instruction Point of Contact.....	4
Support Systems.....	4
Process Narrative.....	5
Process Flow Diagram.....	7
Table 1: Risk & Internal Control Table.....	8
SECTION III - CONFIGURATION CONTROL.....	8
APPROVING SIGNATURE.....	8
APPENDIX A - PROCESS FLOW DIAGRAM LEGEND.....	9
APPENDIX B - ACRONYM LIST AND GLOSSARY.....	10
APPENDIX C - REFERENCES/AUTHORITIES.....	13

NI 56-2-2, Prepublication Review
FY 2013

56-2-2 CHANGE LOG

(b)(3) 10 USC 1424

Revision	Date	Revised By	Pages Affected	Remarks
1.0	26 Feb 2013	<input type="text"/>	ALL	Updated to realign with NBF50 and reflect organizational changes.
2.0	10 FEB 16	COMM <input type="text"/>	10-12	Administratively updated Glossary and Acronym lists with the Defining IT definitions.

NI 56-2-2, Prepublication Review
FY 2013

SECTION I - INTRODUCTION

In accordance with the National Reconnaissance Office (NRO) Governance Plan, NRO Business Function (NBF) 50, Information Technology, Information Assurance, and Information Management (IT-IA-IM) and NRO Directive 56-2, this NRO Instruction (NI) sets forth the procedural implementation guidance and provides applicable information to perform the Prepublication Review process. All NRO personnel who perform tasks or have duties specific to Prepublication Review will comply with this NI. When the work to be performed under an NRO contract must comply with this NI, the program office shall list this NI as a reference document in the contract statement of work.

SECTION II - NBF 50 PREPUBLICATION REVIEW SUB-PROCESS DOCUMENTATION

The sub-sections that follow detail the Prepublication Review processing sub-process.

Governing NBF

NBF 50, IT-IA-IM

Description

The Chief Information Officer (CIO) administers the process for approval for public release of any unclassified information (including hard copy, electronic, or verbal) about, or affecting the plans, policies, programs, or operations of the NRO, the Intelligence Community (IC), or the United States Government. This NI provides guidance on when a prepublication review is required and explains the steps that all individuals and components involved in the process must complete. This NI does not apply to the public release of NRO logos or memorabilia. The Office of Security and Counterintelligence (OS&CI) administers a separate process for review and release of logos and memorabilia.

Instruction Point of Contact

Chief, Information Access and Review Team, Information Management Services Office (IMSO), CIO, Secure [REDACTED] (b)(3) 10 USC § 424

Support Systems

IMSO Website - contains additional information in support of the Prepublication Review process.

Prepublication Review Submission System - Enterprise database used by submitters with NRO Management Information System access to request Prepublication Review of unclassified information proposed for public release.

Tracking Information and Enterprise Response (TIER) - Enterprise action tracker used to administer Prepublication Review cases, to include dissemination of information for review, receipt of

**NI 56-2-2, Prepublication Review
FY 2013**

review responses, and case tracking/record-keeping; and used by component for subtasking within components.

Process Narrative

Unclassified materials proposed for public release must have the approval of a Program Security Officer (PSO) and the component supervisory chain prior to sending any materials to the CIO. If NRO contract information or information derived from an NRO contract is included in the material submitted for prepublication review, approval must also be obtained from the Contracting Officer (CO). The CIO will not begin the Prepublication Review process without the required originating component approvals.

A minimum of 20 working days is required for the Prepublication Review process. Submissions that require consultation with external agencies will require additional time. In the event that the CIO is not allowed sufficient time to complete the review process, the CIO will issue a nonconcur determination until such time as the review process can be completed.

1.0 Submitter prepares document for public release and collects necessary approvals.

1.1 The PSO reviews for classified or unclassified sensitive information relating to the submitting office's programs and operations; ensures that the proposed use is a public release; and assists the submitter in resolution of any issues identified in the PSO review.

1.2 The submitter's supervisor and Program Manager (may be the same individual) certify that they are aware of the proposed public release and approve the submission to the CIO for further processing. This step is not required for resumes.

1.3 If the materials proposed for public release are related to an NRO contract, the cognizant CO reviews the submission and certifies that the release does not violate the NRO Acquisition Manual terms regarding public release of contract-related information.

2.0 Author submits the final draft of the unclassified materials proposed for public release along with your component approvals to the CIO to begin the prepublication review process a full 20 working days before the due date.

3.0 Materials must be resubmitted for review if any changes are made to the drafts after submission other than editorial, grammatical, or those recommended by CIO.

4.0 Contact the CIO immediately if unusual circumstances prevent drafts from being submitted in time to meet

**NI 56-2-2, Prepublication Review
FY 2013**

submission deadlines. CIO will not expedite non-official publications.

5.0 Upon receipt of the unclassified materials for Prepublication Review and the required component approvals, the CIO will analyze the submission and task the appropriate directorates and/or offices to review the materials. OS&CI/Policy, Office of Strategic Communications (Public Affairs), and Advanced Systems & Technology Directorate will review all submissions other than resumes. (b)(3) 10 USC 424

5.1 Components tasked with review will administer the review process within the individual components, utilizing cognizant PSOs and/or subject matter experts. The review process is determined by the individual components.

5.2 Components compile and consolidate component-internal review findings into a single component-level response to the CIO and respond to the TIER action on behalf of the reviewing component. The component TIER response must include a clear statement of concurrence, nonconcurrence, or concurrence with comment. In the event of a nonconcurrence, the component response must include a clear explanation as to the reasons for the nonconcurrence and, if possible, a recommendation for change that would be acceptable.

6.0 Upon completion of NRO component reviews, the CIO will make a determination regarding the necessity for review by other agencies.

6.1 For official NRO releases, the CIO will consult with other agencies as appropriate as part of this process. Additional time is needed for external consultation. If external consultation is required for an official NRO release, the CIO will not issue a final release determination until consultation responses are received in the CIO.

6.2 For non-NRO releases, the CIO does not administer external consultations as part of this process, but will advise the submitter in this regard as part of the final review determination response.

7.0 After all component and external reviews are complete, the CIO will respond to the submitter with a release determination, to include guidance on the conditions under which the materials may be released to the public, a detailed accounting of any revisions that must be made before public release, or approval for the release of the materials as submitted.

8.0 The submitting office has sole responsibility for maintaining a copy of the approval to release the information. It should be kept with the submission and maintained in accordance with the NRO Record Control Schedule.

NI 56-2-2, Prepublication Review
FY 2013

Process Flow Diagram

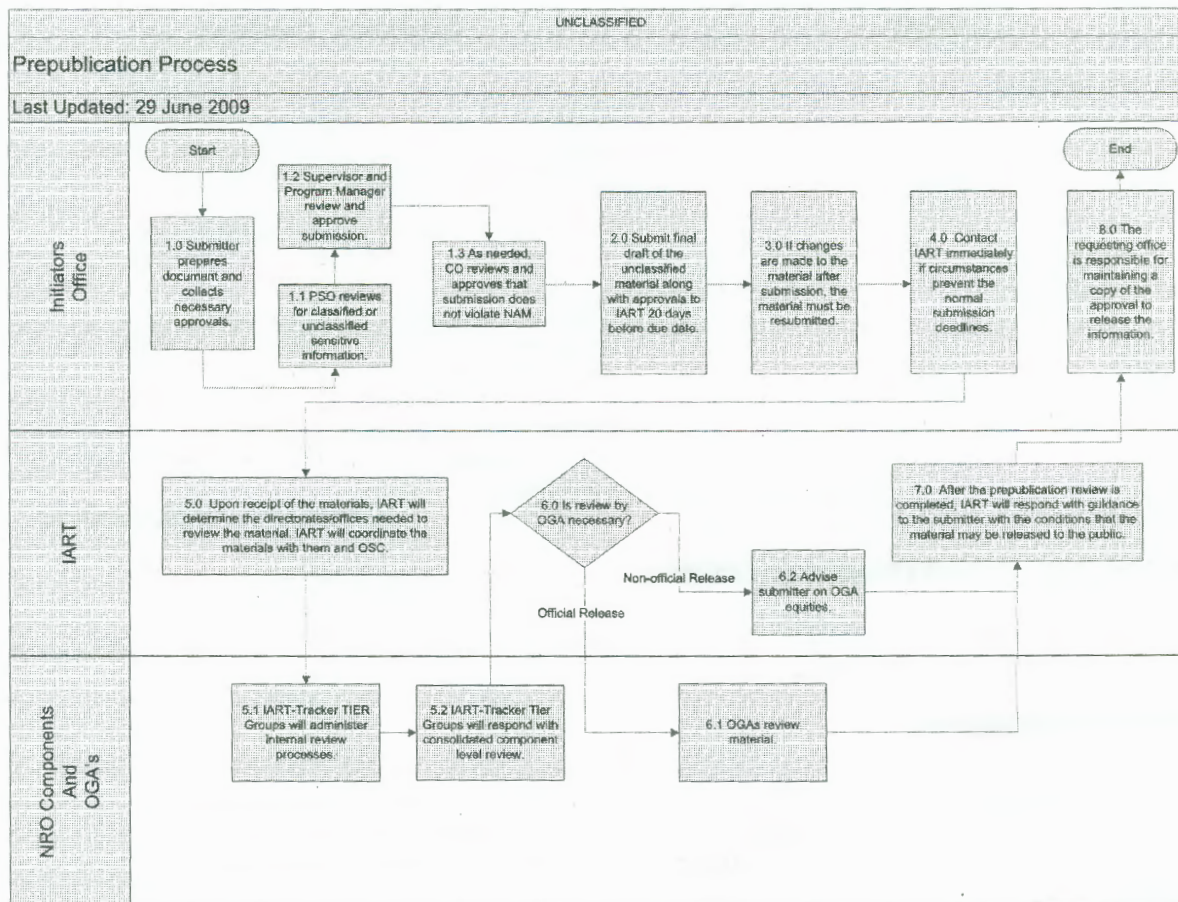


Figure is UNCLASSIFIED

NI 56-2-2, Prepublication Review
FY 2013

Table 1: Risk & Internal Control Table

Risk	Internal Control
Inadvertent release of information not appropriate for the public.	All unclassified materials proposed for release to the public must be submitted to the PSO and component supervisory chain for approval prior to materials being sent to CIO. CIO tasks appropriate Directorates and Offices to review the material. CIO determines if Department of Defense or the IC needs to review the material prior to release. Documented agreement with IC counterparts to assist in reviewing equities.

Table is UNCLASSIFIED

SECTION III - CONFIGURATION CONTROL

All changes to the IT-IA-IM, Prepublication Review Instruction require NBF owner approval.

APPROVING SIGNATURE

As the NBF owner for IT-IA-IM, I confirm that this document provides a complete representation of the Prepublication Review Instruction, and that the document has been coordinated with stakeholders of the process.

Jim T. Singer

Jim T. Singer
IT-IA-IM NBF Owner

26 Feb 2013

Date

NI 56-2-2, Prepublication Review
FY 2013

APPENDIX A - PROCESS FLOW DIAGRAM LEGEND



Figure is UNCLASSIFIED

NI 56-2-2, Prepublication Review
FY 2013

APPENDIX B - GLOSSARY

Term	Definition
Agency	Any executive or military department, other establishment, or entity included in the definition of agency in 5 U.S.C. § 522(f).
Business Information Technology	<p>Information Technology (IT) activities associated with the development and maintenance of software and hardware to support business functions to include, but not limited to, human capital, core financials, acquisition, procurement, logistics, grants, asset management, payroll, budget formulation and execution, performance management, travel, time and attendance, cost accounting, project accounting, earned value management, personnel management applications, and elements of security systems that track personnel.</p> <p>Business Information Technology (BIT) also includes all supporting feeder systems that support the Business Management operations of an organization or agency. BIT applications and services shall be available to business systems users via Enterprise Information Technology (EIT) networks and workstations.</p>
Component	Any individual NRO D or O that participates in the Prepublication Review process.
Enterprise Information Technology	Encompasses Information Technology (IT) activities associated with the Agency's infrastructure, such as desktops, local area networks, wide area networks, processors, software, security, operations, help desks, applications, support services, and resources associated with the IT. This category identifies IT elements and applications available to all users of the enterprise (e.g., e-mail). Information assurance (IA) capabilities are to be included in this category. Also included in the Enterprise Information Technology (EIT) category are completely installed computer systems and their peripheral components.

NI 56-2-2, Prepublication Review
FY 2013

Term	Definition
Information Technology	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Equipment is used directly or is used by a contractor under a contract which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information Technology (IT) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It is further delineated by Business Information Technology (BIT), Enterprise Information Technology (EIT), and Mission Information Technology (MIT).
Mission Information Technology	Information Technology (IT) activities associated with collection, analysis, and production systems, and information sharing/collaboration tools, applications, and software, with the exception of office automation systems. These systems can exist at the point where information is initially processed or at the point where analysts turn collected information into intelligence and knowledge. Mission Information Technology (MIT) also includes special purpose software and IT elements used among small, unique user populations.
Non-NRO Release	A record or document that will be released not on the behalf of the NRO (for example, private party documents, contractor produced documents not produced for the NRO).
Official Release	A record or document that will be released by the NRO or an NRO component as part of its mission and function
Prepublication Review	The process established to control and monitor the release of unclassified information about, or affecting the plans, policies, programs, or operations of the NRO, the Intelligence Community or U.S. Government.
Submitter	The individual who created the document at issue.
Working Days	Days when the NRO is operating (specifically excludes Saturdays, Sundays, and legal public holidays).

Table is UNCLASSIFIED

NI 56-2-2, Prepublication Review
FY 2013

APPENDIX B - ACRONYM LIST

Term	Definition
BIT	Business Information Technology
CIO	Chief Information Officer
CO	Contracting Officer
EIT	Enterprise Information Technology
IC	Intelligence Community
IMSO	Information Management Services Office
IT	Information Technology
IT-IA-IM	Information Technology, Information Assurance, Information Management
MIT	Mission Information Technology
NBF	NRO Business Function
NI	NRO Instruction
NRO	National Reconnaissance Office
OS&CI	Office of Security and Counter-Intelligence
PSO	Program Security Officer
TIER	Tracking Information and Enterprise Response

Table is UNCLASSIFIED

NI 56-2-2, Prepublication Review
FY 2013

APPENDIX C - REFERENCES/AUTHORITIES

- a. 50 United States Code, Chapter 15, National Security Act of 1947
- b. Executive Order 12333, United States Intelligence Activities, as amended
- c. Executive Order 13526, Classified National Security Information, 29 Dec 09
- d. Department of Defense Instruction 5230.29, Security and Policy Review of Department of Defense Information for Public Release, 8 Jan 09
- e. Department of Defense Regulation 5230.9, Clearance of Information for Public Release, 9 Apr 96 (b)(3) 50 USC + 3507
- f. Agency Regulation [] Agency Prepublication Review of Certain Material Prepared for Public Dissemination, 30 May 07
- g. Agency Regulation [] Policy and Procedures for the Release of Unclassified Agency Official Information to the Public, 19 Sep 95
- h. National Reconnaissance Office Acquisition Manual
- i. National Reconnaissance Office Business Function 50, Information Technology, Information Assurance, and Information Management
- j. National Reconnaissance Office Directive 56-2, Access and Release



**NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY 1-30**



Issue Date: 13 May 2015
Revised: 12 May 2017

REVIEW OF NSA/CSS INFORMATION INTENDED FOR PUBLIC RELEASE

PURPOSE AND SCOPE

This document sets forth the policy, procedures, and responsibilities governing the prepublication review of official NSA/CSS information intended for public release by current and former NSA/CSS affiliates in either an official capacity or a private capacity. This policy also implements Department of Defense (DoD) Directive 5230.09, "Clearance of DoD Information for Public Release" (Reference a).

This policy applies to all current and former NSA/CSS affiliates and reflects lifetime obligations agreed to in non-disclosure agreements.

/s/

ELIZABETH R. BROOKS
Chief of Staff

/s/

Endorsed by
Associate Director for Policy

Policy 1-30 is approved for public release.

000088

Policy 1-30

Dated: 13 May 2015

DISTRIBUTION:

P12
P13
P131
P134 (Vital Records)

This Policy supersedes NSA/CSS Policy 1-30 dated 10 May 2013. The Chief, Policy approved an administrative update on 12 May 2017 to update organizational designators for NSA21. OPI: Information Security and Classification Division, P131, 972-2534 (secure) or (443)-634-4094 (non-secure).

POLICY

1. Public release in an official capacity:

a. NSA/CSS makes certain accurate and timely information available to the public to promote accountability for and understanding of its activities. The public release of official NSA/CSS information shall be limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate Government interest ([Reference a](#)). All current NSA/CSS affiliates shall submit for prepublication review all official NSA/CSS information intended for public release in their official capacity. The prepublication review process includes both a classification review and a review that determines whether the information intended for public release: is consistent with established NSA/CSS, DoD, and Intelligence Community policies and programs; is consistent with information security standards established by the Office of Information Management (OIM, P13); and conforms to NSA/CSS corporate messaging standards as determined by Strategic Communications (P2).

b. Official NSA/CSS information prepared as part of official duties and approved for public release will be used in accordance with DoD Directive (DoDD) 5500.07, "Standards of Conduct" ([Reference b](#)), and DoD 5500.7-R, "Joint Ethics Regulation (JER)" ([Reference c](#)), which preclude such use for monetary or nonmonetary personal gain.

2. Public release in a private capacity: NSA/CSS affiliates acting in a private capacity, and not in connection with their official duties, may prepare information for public release without management approval or policy review provided that the affiliate:

- a. Violates no laws or regulations;
- b. Maintains ethical standards and compliance with [References b and c](#);
- c. Uses only information that is UNCLASSIFIED and approved for public release;
- d. Uses no information in which NSA/CSS may have intellectual property rights and must file a new patent application with the U.S. Patent and Trademark Office thereon

Policy 1-30

Dated: 13 May 2015

or lose the right to do so (i.e., the information, if publicly released, does not establish a date by which NSA/CSS must file a new patent application (e.g., 1 year after public release)); and

e. Uses a disclaimer on any material in which an NSA/CSS affiliation is cited, stating that the views and opinions expressed are those of the affiliate and do not reflect those of NSA/CSS.

3. Information available from both classified and open sources:

a. Official NSA/CSS information appearing in the public domain shall not be automatically considered UNCLASSIFIED or approved for public release.

b. Where information intended for public release is available to the NSA/CSS affiliate from classified sources and also independently from open sources, the affiliate may be permitted to release the information if the affiliate can cite an adequate open-source publication where the specific information is available – only if release of the information by the affiliate at the time of review will not cause additional damage to national security through confirmation of previous unauthorized releases. The appropriate Prepublication Review Authority shall exercise discretion in making such determinations on a case-by-case basis and may consider the following as factors in the decision:

- 1) The sensitivity of the information from classified sources;
- 2) The number and currency of the previous releases;
- 3) The level of detail previously exposed;
- 4) The source of the previous releases (whether authoritative and acknowledged or an anonymous leak);
- 5) The submitter's access to classified sources; and
- 6) The authority and credibility afforded by the affiliate's NSA/CSS experience.

4. Official NSA/CSS organizational logos: A logo may be *created* in accordance with NSA/CSS Policy 10-7, "NSA/CSS Multimedia Information" (Reference d). Once Graphics Services (P2212) creates a proof of the logo, it must be reviewed and approved for public release in an official capacity as set forth in this policy. Once approved for public release, a logo may be used for official NSA/CSS operational, promotional, or morale-building purposes.

Policy 1-30

Dated: 13 May 2015

PROCEDURES

5. For public release in official capacity:

a. Information intended for public release in an NSA/CSS affiliate's official capacity (including, but not limited to, books, articles, videos, speeches, conference briefings, Internet postings, biographies, book reviews, cooperative education (co-op) reports, press releases, research papers, and organizational logos) is subject to prepublication review.

b. Before publicly disclosing his or her NSA/CSS affiliation, a current affiliate preparing material for public release in an official capacity shall seek operations security (OPSEC) guidance from his or her Staff Security Officer (SSO) and solicit a [name check](#) from Chief, NSA/CSS Cover Office (X073) in accordance with NSA/CSS Policy 1-18, "NSA/CSS Cover Program" ([Reference e](#)).

c. Whenever practicable, to preclude the inadvertent spillage of classified information onto unclassified systems, NSA/CSS affiliates acting in an official capacity shall use a TOP SECRET classified information system (e.g., NSANet, JWICS) to draft the full material intended for public release. Notes, outlines, or other partial information may not be substituted for the full material intended for public release in order to avoid the possibility of classification due to compilation.

d. Current NSA/CSS affiliates acting in an official capacity shall first submit, for management review and approval, all official NSA/CSS information intended for public release.

e. Upon receipt of management approval for public release (which may be in the form of a digitally signed email), a current NSA/CSS affiliate acting in an official capacity submits the following to a local [Classification Advisory Officer \(CAO\)](#) for an initial classification determination: the full material intended for public release, management approval, and written consent from NSA/CSS affiliates identified in the information to have any NSA/CSS affiliation publicly revealed. A complete list of CAOs can be found on NSANet ("[go cao](#)").

f. Upon determining the information to be UNCLASSIFIED, the CAO sends a digitally signed email to the affiliate containing that determination.

g. Following procedures established by the Prepublication Review Authority, either the affiliate or the local CAO then forwards the full and final material intended for public release (with all classification markings and/or handling instructions removed), management approval, classification determination, written consent from affiliates identified in the information to have any NSA/CSS affiliation publicly revealed (if applicable), technical review (if applicable), and contracting officer approval (if applicable) to the appropriate NSA/CSS Prepublication Review Authority for the final prepublication review determination.

Policy 1-30

Dated: 13 May 2015

h. The appropriate Prepublication Review Authority shall:

- 1) As necessary, coordinate with other information owners should the material contain information not under his or her purview;
- 2) Refer the information for review to organizations external to NSA/CSS, if required;
- 3) Coordinate, as appropriate, a review with the Public Affairs Office (PAO, P21) to determine that information intended for public release in an affiliate's official capacity conforms to NSA/CSS corporate messaging standards;
- 4) When necessary, request a technical review by a subject matter expert to determine that the information intended for public release is accurate;
- 5) When necessary, request a review by the NSA/CSS Office of the General Counsel (OGC) to determine that the information intended for public release contains no information in which NSA/CSS may have intellectual property rights and may file a patent application thereon; and
- 6) If the current NSA/CSS affiliate acting in an official capacity is a Senior Leader, coordinate with the Information Security and Classification Division (P131) to obtain prepublication approval from the Defense Office of Prepublication and Security Review (DOPSR).

i. The appropriate Prepublication Review Authority will issue, as practicable, a final determination to the affiliate within 25 business days of receipt of all required information and supporting documentation.

6. For public release in a private capacity:

a. Resumes, associated cover letters, work-related biographies (bios), and curriculum vitae (CVs) intended for any public use: Current and former NSA/CSS affiliates shall submit résumés, associated cover letters, work-related bios, and CVs intended for public release to the Information Security and Classification Division (P131) for review according to procedures published on the Information Security and Classification Division (P131) Web site and on nsa.gov to determine whether they contain NSA/CSS protected information.

1) Before publicly disclosing his or her NSA/CSS affiliation in such a document, a current affiliate shall seek OPSEC guidance from an SSO and solicit a name check from Chief, X073.

2) Whenever practicable and with supervisory approval, to preclude the inadvertent spillage of classified information onto unclassified systems, current NSA/CSS affiliates acting in a private capacity may use a TOP SECRET classified information system (e.g., NSANet, JWICS) to draft the full version of such documents intended for public release. Notes, outlines, or other partial

Policy 1-30

Dated: 13 May 2015

information may not be substituted for the full material intended for public release in order to avoid the possibility of classification due to compilation.

3) A current affiliate shall have such documents first reviewed by an organizational CAO before submitting it to P131.

4) Former affiliates shall submit such documents per instructions in [paragraph 6.b.4.](#)

5) Résumés are not subject to management approval or policy review.

b. Other than résumés: Current and former NSA/CSS affiliates may prepare material for public release that meets all of the requirements stated in [paragraph 2.](#) This includes, but is not limited to, books, articles, videos, speeches, conference briefings, Internet postings, book reviews, co-op reports, press releases, research papers, and organizational logos. However, prepublication review is required where compliance with the requirements of [paragraph 2](#) is in doubt (i.e., where the material contains official NSA/CSS information that may or may not be UNCLASSIFIED and approved for public release). Before publicly disclosing an NSA/CSS affiliation, a current affiliate shall seek OPSEC guidance from an SSO and solicit a name check from Chief, X073.

1) Whenever practicable and with supervisory approval, to preclude the inadvertent spillage of classified information onto unclassified systems, current NSA/CSS affiliates acting in a private capacity may use a TOP SECRET classified information system (e.g., NSANet, JWICS) to draft the full material intended for public release. Notes, outlines, or other partial information may not be substituted for the full material intended for public release in order to avoid the possibility of classification due to compilation.

2) A current affiliate with access to a TOP SECRET classified network (e.g., NSANet, JWICS) shall request review by his or her organization's CAO of the full material intended for public release. After review, the organization's CAO will send the full and final material and the initial determination to the appropriate Prepublication Review Authority for a second review.

3) Current affiliates without access to a TOP SECRET classified network (e.g., NSANet, JWICS) may submit the full and final material intended for public release via another classified system (e.g., SIPRNet) to the appropriate Prepublication Review Authority according to established procedures.

4) Former affiliates without access to a TOP SECRET classified network (e.g., NSANet, JWICS) shall submit the full and final material intended for public release in hardcopy to:

NSA/CSS
ATTN: P131, Prepublication Review
9800 Savage Road

Policy 1-30

Dated: 13 May 2015

Suite 6932

Fort George G. Meade, MD 20755-6248

5) The appropriate Prepublication Review Authority shall create an official record of the documents reviewed and the determinations made.

6) As necessary, the appropriate Prepublication Review Authority shall coordinate with other information owners when the material contains information under their purview.

7) The appropriate Prepublication Review Authority shall, as practicable, issue the determination to the affiliate within 25 business days of receipt.

7. Appeal of a prepublication review determination:

a. A prepublication review determination may be appealed in writing to the Chief, OIM within 20 business days of receipt of the determination. At OIM's discretion, an additional 30 business days may be allowed to file a written appeal, provided that the affiliate files a written notice of intent to appeal within 20 business days of receipt of the initial determination and presents justification to support an extension. The affiliate making the appeal shall specifically identify the disputed portions of the initial determination and the reasons for appeal – and shall include any supporting information that the Chief, OIM should consider.

b. In support of OIM, the Information Security and Classification Division (P131) will, if necessary, schedule meetings with the NSA OGC and/or the information owners to review the disputed information and, within 30 business days of receipt of the appeal, advise the affiliate making the appeal of the Chief's OIM final determination and, to the extent consistent with national security, the reasons for any OIM determination adverse to the affiliate's interests.

c. The final determination by the Chief, OIM may not be further appealed.

RESPONSIBILITIES

8. A current NSA/CSS affiliate acting in an official capacity shall:

a. Before disclosing his or her NSA/CSS affiliation, solicit a name check from Chief, X073 in accordance with [Reference e](#);

b. Seek OPSEC guidance from an SSO regarding the possible consequences of disclosing his or her NSA/CSS affiliation;

c. Submit for prepublication review all materials intended for public release according to the procedures specified in [paragraph 5](#);

Policy 1-30

Dated: 13 May 2015

d. As applicable, obtain written consent from each affiliate identified in the information to have his or her NSA/CSS affiliation publicly revealed; and

e. In accordance with established procedures, submit to the appropriate Prepublication Review Authority his or her requests for prepublication review along with all required information identified in [paragraph 5.g.](#).

9. Current NSA/CSS affiliates acting in a private capacity shall:

a. Before disclosing their NSA/CSS affiliation, solicit name checks from Chief, X073 in accordance with [Reference e](#);

b. Seek OPSEC guidance from an SSO regarding the possible consequences of disclosing their NSA/CSS affiliation;

10. Current and former NSA/CSS affiliates acting in a private capacity shall:

a. Submit for prepublication review all materials intended for public release according to the procedures specified in [paragraph 6](#);

b. Notify NSA/CSS of any request to comment on any unofficial NSA/CSS-related information (e.g., to review a book by a non-Government author prior to publication, to review an article). The NSA/CSS affiliate shall regard his/her comments as a proposed unofficial publication subject to review, as provided by this policy. If the appropriate Prepublication Review Authority determines that all or part of the text being commented on must be reviewed in order to evaluate the comments, the affiliate shall obtain permission from the author before submitting relevant parts of any unpublished text to NSA/CSS for review; and

c. As applicable, obtain written consent from each affiliate identified in the information to have his or her NSA/CSS affiliation publicly revealed.

11. Classification Advisory Officers (CAOs) shall:

a. Conduct an initial classification review of information submitted by an affiliate in their supported organizations, in accordance with current NSA/CSS classification and declassification guidance;

b. Provide the affiliate with a digitally signed email message or, if email is not practicable, an appropriately classified letter containing the classification determination; and

c. In accordance with established procedures and on behalf of the affiliate, submit a request for prepublication review to the appropriate Prepublication Review Authority (see [paragraph 5.g.](#)).

Policy 1-30

Dated: 13 May 2015

12. Prepublication Review Authorities shall:

- a. Assist the CAO, when necessary, in resolving classification disputes;
- b. Coordinate reviews, as appropriate, with PAO for conformance to messaging standards;
- c. If the current NSA/CSS affiliate acting in an official capacity is a Senior Leader, coordinate with the Information Security and Classification Division (P131) to obtain prepublication approval from the DOPSR;
- d. Coordinate prepublication reviews with any other NSA/CSS offices as required by, and specified in, this policy;
- e. Coordinate prepublication reviews with external information owners (e.g., U.S. Government, foreign government), as appropriate;
- f. Conduct, as practicable, final prepublication reviews of all information intended for public release within 25 business days of receipt;
- g. Notify the affiliate in writing of the determination; and
- h. Maintain all required electronic and hardcopy official records related to prepublication review determinations in accordance with this policy and NSA/CSS Policy 1-6, "Records Management Program" ([Reference f](#));

13. The Information Security and Classification Division (P131) shall perform all of the functions of a Prepublication Review Authority (see [paragraph 12](#)) and shall:

- a. Serve as the sole approval authority for the public release of personal résumés;
- b. Coordinate with the DOPSR to obtain public release approval when the current NSA/CSS affiliate acting in an official capacity is a Senior Leader;
- c. Review and approve or disapprove management directives and any other procedures developed to implement this policy;
- d. Maintain accountability and a database for all required electronic and hardcopy official records related to prepublication review determinations in accordance with [Reference f](#); and
- e. Administratively assist the Chief, OIM in the processing of prepublication review appeals.

14. The Research Director, in addition to the responsibilities in [paragraph 15](#), shall:

- a. Issue management directives to implement this policy that have been approved by the Information Security and Classification Division (P131);

Policy 1-30

Dated: 13 May 2015

b. Provide a monthly accounting of prepublication review cases to the Information Security and Classification Division (P131); and

c. Grant the Information Security and Classification Division (P131) access to any databases used for the electronic storage and tracking of prepublication review cases.

15. The Directors, Cryptologic Center Commanders/Chiefs, and Field Commanders/Chiefs shall:

a. Develop a process, consistent with the provisions in this policy, for ensuring the proper prepublication review of official NSA/CSS information intended for public release;

b. Ensure that personnel under their supervision are made aware of the requirements of this policy; and

c. Ensure that subordinates' requests for management review and approval of official NSA/CSS information intended for public release pursuant to [paragraph 5.b](#) are completed in a timely manner.

16. The Security and Counterintelligence Group (A5) shall:

a. Ensure that, during initial indoctrination, all affiliates are informed of their lifelong responsibility to safeguard NSA/CSS protected information and of the procedures for prepublication review;

b. Ensure that all affiliates are reminded of their lifetime prepublication review responsibilities prior to signing their security debriefing forms at the end of their affiliation with the Agency; and

c. Via SSOs, provide OPSEC guidance to current affiliates regarding the possible consequences of publicly disclosing their NSA/CSS affiliation when preparing official NSA/CSS information for public release in either an official or private capacity.

17. The Office of General Counsel (OGC) shall:

a. Provide legal advice to a Prepublication Review Authority when material intended for public release contains any information in which NSA/CSS may have intellectual property rights and may file a patent application thereon;

b. Ensure, in coordination with the Business Management and Acquisition Directorate (B), that contracts contain necessary provisions to require compliance with the provisions of this policy by contractors and their employees; and

c. Provide legal advice and guidance to the Information Security and Classification Division (P131) and Chief, OIM during the appeal process, as necessary and as required.

Policy 1-30

Dated: 13 May 2015

18. The Business Management and Acquisition Directorate (BM&A) shall ensure, in coordination with the OGC, that contracts contain necessary provisions to require compliance with the provisions of this policy by contractors and their employees.

19. The Public Affairs Office (PAO) shall, as appropriate, perform a review on all information intended for public release in an official capacity within 10 business days of receipt to ensure that information intended for public release conforms to current NSA/CSS messaging standards as determined by Strategic Communications.

20. The Chief, NSA/CSS Cover Office (X073) shall conduct name checks as requested by current affiliates preparing official NSA/CSS information for public release in either an official or private capacity in accordance with [Reference e.](#)

REFERENCES

21. References:

- a. [DoDD 5230.09](#) "Clearance of DoD Information for Public Release," dated 22 August 2008.
- b. [DoDD 5500.07](#), "Standards of Conduct," dated 29 November 2007.
- c. [DoD 5500.7-R](#), "Joint Ethics Regulation (JER)," dated 1 August 1993.
- d. [NSA/CSS Policy 10-7](#), "NSA/CSS Multimedia Information," dated 12 August 2009 and revised 1 May 2013.
- e. [NSA/CSS Policy 1-18](#), "NSA/CSS Cover Program," dated 6 March 2014.
- f. [NSA/CSS Policy 1-6](#), "Records Management Program," dated 19 November 2014.
- g. [Executive Order 13526](#), "Classified National Security Information," dated 25 January 2010.
- h. [Public Law No. 86-36](#) (codified as amended in 50 U.S.C. § 3605), "National Security Agency Act of 1959."
- i. [5 U.S.C § 552](#), "Freedom of Information Act."

DEFINITIONS

22. [Affiliate](#) – A person employed by, detailed to, or assigned to NSA/CSS, including a member of the U.S. Armed Forces; an expert or consultant to NSA; an industrial or commercial contractor, licensee, certificate holder, or grantee of NSA, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of NSA/CSS as determined by the Director, NSA/Chief, CSS. (Source: [NSA/CSS Policy Glossary](#))

Policy 1-30

Dated: 13 May 2015

23. Classification Advisory Officer (CAO) – An individual trained to properly apply classification rules and guidance and who assists other employees in the proper marking and protection of classified and protected information. The Information Policy and Classification Division (P131) administers the CAO Program and registers CAOs. For more information “go CAO.”

24. Logo – An unclassified graphical representation of an NSA/CSS-related special office, mission, program, or project.

25. Name Check – A review of past assignments, including assignments to other agencies and participation in educational programs, to determine the classification of an individual’s name in association with NSA/CSS ([Reference e](#)).

26. Nondisclosure Agreement (NdA) – A lifetime obligation to safeguard all protected information, to submit all information intended for publication and/or public release for prepublication review, and to report any unauthorized disclosure of protected information. NSA/CSS affiliates are legally bound and obligated by any NdAs they sign for access to NSA/CSS information. They shall not confirm or deny information about NSA/CSS that appears in the public domain without prior approval through the classification or prepublication process.

27. NSA/CSS Protected Information – Information obtained as a result of a relationship with NSA/CSS, that is:

a. Classified or in the process of a classification determination pursuant to the standards of Executive Order 13526 ([Reference g](#)), or any successor order, and implementing regulations. It includes, but is not limited to, intelligence information, sensitive compartmented information (intelligence sources and methods), and cryptologic information (information concerning information systems security and signals intelligence); or

b. Unclassified, appearing in any form or compilation, which NSA/CSS may withhold from public disclosure under authority of the National Security Agency Act of 1959 ([Reference h](#)) or by reason of being either excluded or exempted from the mandatory disclosure requirements of the Freedom of Information Act ([Reference i](#)).
(Source: [NSA/CSS Policy Glossary](#))

28. Official Capacity – Acting on behalf of NSA/CSS.

29. Official NSA/CSS Information – Any NSA/CSS, DoD, or IC information that is in the custody and control of NSA/CSS and was obtained for or generated on NSA/CSS’ behalf during the course of employment or other service, whether contractual or not, with NSA/CSS.

30. Prepublication Review – The overall process to determine that information proposed for public release contains no protected information and, where applicable, is consistent with established NSA/CSS, DoD, and IC policies and programs; conforms to NSA/CSS messaging standards as determined by Strategic Communications; and, in consultation with the NSA OGC,

Policy 1-30

Dated: 13 May 2015

Acquisition, Research, and Technology Law Practice, as appropriate, contains no information in which NSA/CSS may have intellectual property rights and may file a patent application thereon.

31. Prepublication Review Authority – Officials in organizations who are delegated the authority to make determinations on prepublication reviews. The Information Security and Classification Division (P131) serves as the corporate-level Prepublication Review Authority and as such has the authority to make a determination on any prepublication review and has sole authority for the prepublication review of personal résumés, associated cover letters, bios, and CVs. The Chief, Office of Information Management (OIM, P13) has officially delegated Prepublication Review Authority to the Research Directorate for review of RD-related, non-résumé material and/or non-résumé material submitted by RD personnel.

32. Private Capacity – Acting on behalf of oneself and not in association with NSA/CSS.

33. Public Release – The decision to give permission to retain, or to show or reveal official NSA/CSS information whether orally, in writing, or through any other medium, to one or more persons who otherwise do not have the appropriate access authorization, security clearance, and/or need to know to receive such information upon determination that the release will not harm the national security or another legitimate Government interest.

34. Senior Leader – A Defense Intelligence Senior Executive Service (DISES) employee, a Defense Intelligence Senior Level (DISL) employee, or the military equivalent of a DISES or DISL employee.

35. Unauthorized Disclosure – Absent a public release, the communication or physical transfer of protected information to one or more unauthorized recipients who do not have appropriate access authorization, security clearance, and/or need to know to receive such information.

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INSTRUCTION NO. 2007-6**

SUBJECT: THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE INSTRUCTION FOR ODNI PRE-PUBLICATION REVIEW OF MATERIAL PREPARED FOR PUBLIC DISSEMINATION

1. AUTHORITY: The National Security Act, as amended; Executive Orders 12333 and 12958, as amended; Freedom of Information Act (FOIA); and The Privacy Act of 1974, as amended, and other applicable provisions of law.

2. PURPOSE:

A. Consistent with the Office of the Director of National Intelligence (ODNI) intent to improve outreach to academia, industry, and the public at large, this instruction establishes the requirements and process for review of materials prepared by persons covered by this instruction for unofficial publication or other forms of unofficial public dissemination to ensure the protection of classified information and, for current staff, assignees, detailees, and contractors, additional interests as outlined below. While the ODNI encourages outreach, this policy does not release persons from the obligation to fully comply with nondisclosure agreements or other secrecy agreements or alter the terms of such agreements. In case of any conflict between this document and a nondisclosure agreement or other secrecy agreement, the nondisclosure agreement or other secrecy agreement shall govern.

B. Pre-publication review is intended to prevent the disclosure of classified information, and, for current staff, assignees, detailees, and contractors, to ensure that neither the author's performance of duties, the ODNI's mission, nor the foreign relations or security of the U.S. are adversely affected by publication. This instruction supersedes CIA Regulation (AR) 6-2, as it applies to the ODNI. A separate Instruction to cover official publications and presentation will be issued at a later date.

3. APPLICABILITY: This instruction applies to all individuals granted access to classified information by the ODNI or who sign a nondisclosure agreement or other secrecy agreement, including current and former staff, assignees, detailees and contractors. Current and former assignees and detailees from home agencies that have a pre-publication review process shall submit materials to their home agency for review and provide notice to the ODNI as set out in paragraph 5.B. below.

UNCLASSIFIED
000101

UNCLASSIFIED

4. POLICY: Each individual granted access to classified information by the ODNI or who signs a nondisclosure agreement or other secrecy agreement shall submit to the ODNI, for prepublication review and approval in accordance with this Instruction. All materials intended for unofficial publication or unofficial public dissemination, whether they will be communicated in writing, speeches, electronically, or by any other method, that mention the ODNI, elements of the Intelligence Community (IC), or intelligence data or activity shall be submitted.

A. Materials must be submitted at each stage of their development prior to being circulated to anyone who does not have the requisite clearance. Circulating materials prior to completing the ODNI prepublication review process violates this instruction and the author's prepublication review obligation and ODNI reserves the right to conduct a post-publication review of any such material in order to take any necessary protective action to mitigate damage caused by such a disclosure.

B. In informal situations where no prepared remarks are delivered, each individual granted access to classified information by the ODNI or who signs a nondisclosure agreement or other secrecy agreement is responsible for remaining within the guidelines provided above.

C. When a co-author who has not signed an ODNI nondisclosure agreement or other secrecy agreement will contribute to a publication subject to pre-publication review, each version of the publication submitted for pre-publication review must clearly identify those portions of the publication that were authored by the individual with access to classified information or subject to the nondisclosure agreement or other secrecy agreement. Where there is any ambiguity concerning which individual wrote a section, and the section was not submitted for review, ODNI reserves the right to consider the section to be entirely written by the individual subject to the nondisclosure agreement or other secrecy agreement and therefore in violation of the individual's pre-publication review obligations.

D. The pre-publication review requirement does not apply to material that is unrelated to intelligence or to ODNI employment or contract matters (for example, material that relates to cooking, stamp collecting, sports, fraternal organizations, and so forth).

5. ROLES AND RESPONSIBILITIES:

A. **Current staff and contractors** covered by this policy are required to submit materials to the Director, Information Management Office (IMO). Requestors may seek one-time approval of publications related to recurring activities.

B. **Current and former assignees and detailees** whose home agency has a pre-publication review process shall submit materials to their home agency for review and provide notice to the Director, IMO. They do not need to submit their materials directly to the Director, IMO.

UNCLASSIFIED

C. Current Supervisor: In the case of current staff and contractors, the requestor's supervisor will provide the initial pre-publication review, and recommended disposition, to the Director, IMO. In reviewing the submission, the supervisor will apply the criteria applicable to current staff and contractors, as described below.

D. Public Affairs Office (PAO): PAO will be notified by the Director, IMO of all materials submitted for public dissemination. PAO will review all materials, particularly those that may be of interest to the media, and will provide a recommendation to the Director, IMO.

E. Director, Information Management Office:

(1) The Director, IMO is the central point for all requests submitted by current ODNI staff and contractors, current and former assignees and detailees whose home agency does not have a pre-publication review process, and former ODNI staff and contractors. The Director, IMO will prioritize and refer requests to other ODNI organizations including but not limited to the Deputy Directors and Mission Managers, PAO, the Office of General Counsel, and other offices as appropriate. Copies should not be circulated beyond those officials participating directly in the process. The Director, IMO will maintain records of all pre-publication review requests and actions. The Director, IMO will monitor pre-publication review cases, and assist applicants with problems, helping to track cases in progress and provide final guidance to the requestor.

Standard for review:

- (a) For former staff and contractors and former assignees and detailees whose home agency does not have a pre-publication review process, material proposed for publication or public dissemination will be reviewed solely to determine whether it contains any classified information. Permission to publish will not be denied because the material may be embarrassing to or critical of the ODNI or the IC.
 - (b) For current staff and contractors and current assignees and detailees whose home agency does not have a pre-publication review process, in addition to the prohibition on revealing classified information, the Director, IMO may deny permission to publish materials that could
 - a. Reasonably be expected to impair the author's performance of his or her job duties,
 - b. Interfere with the authorized functions of the ODNI, or
 - c. Have an adverse effect on the foreign relations or security of the U.S.
- (2) If any ODNI organization objects to the publication of some or all of the materials submitted, the IMO will work with the objecting organization to determine which portions of the material submitted will be approved for publication. If resolution between the Director, IMO and the objecting organization cannot be reached, the Director, IMO shall refer the question to the Principal Deputy Director of National Intelligence (PDDNI) for final resolution.

UNCLASSIFIED

(3) The Director, IMO will respond to the requestor as expeditiously as possible taking into account the time sensitive nature of the submission, but not later than 30 days from the date of submission. If the Director, IMO cannot meet the 30-day deadline, the requestor will be notified of a new decision date. The Director, IMO's failure to respond to the requestor within 30 days does not constitute approval/clearance and the obligation to submit to pre-publication review is not satisfied until a response is actually received from the Director, IMO.

F. Former staff and contractors and former assignees and detailees whose home agency does not have a pre-publication review process: Questions regarding submission and/or requests from former staff, and contractors and from former assignees and detailees whose home agency does not have a pre-publication review process should be submitted as follows:

E-mail – publicationreview@dni.gov

Fax – 703-482-2144 (ATTN. Director, Information Management Office)

Mail – Director, Information Management Office

Office of the Director of National Intelligence

Washington DC, 20511

(1) When materials are particularly time-sensitive, the requestor should note the time constraints in the approval request and every effort will be made to meet them.

(2) Requestors must not submit possibly classified information using the methods described above. Such information must be treated as classified and the requestor must make appropriate arrangements with the IMO to properly submit such materials.

6. REQUIRED DISCLAIMER:

A. Approval for publication does not imply endorsement. The following disclaimer must be provided in intelligence-related publications created by current ODNI staff and contractors and by current assignees and detailees whose home agency does not have a pre-publication review process when they are acting in their personal capacity:

"The views expressed in (this publication/these remarks) are my own and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. Government agency."

B. Former ODNI staff, assignees, detailees and contractors are not required to provide this disclaimer, as it is understood they do not speak for the ODNI.

7. OTHER PRE-PUBLICATION OBLIGATIONS: This instruction does not supersede any other U.S. Government policy regarding pre-publication review that applies to any staff, assignees, detailees and contractors during their tenure with the ODNI. The Director, IMO will provide guidance to the requestor if additional agency reviews of the material are needed, and any such reviews may take place concurrently

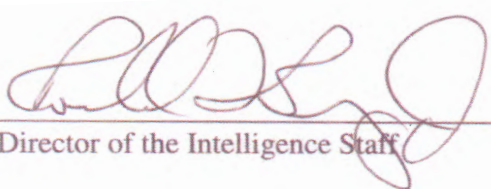
UNCLASSIFIED

with ODNI review. In the case of a conflict between ODNI and agency reviews, the Director, IMO will contact the other agency as soon as possible to obtain a resolution.

8. **APPEALS:** If publication is denied in whole or in part by the ODNI, the Director, IMO must provide the reasons in writing to the requestor. The requestor may then submit additional information and/or revise the draft and request reconsideration. If publication is again denied, the requestor may submit a written appeal within 30 days to the PDDNI; appeal documentation must include the material intended for publication and any supporting materials the appealing party wishes to be considered. A final decision will then be reached by the PDDNI; in consultation with Deputy Directors, Mission Managers or other officials as appropriate. The PDDNI shall issue a written decision on the appeal within 30 days of submission unless additional time is needed.

9. **PENALTY FOR NON-COMPLIANCE:** Failure to comply with prepublication review obligations may result in the imposition of civil and/or administrative penalties.

10. **EFFECTIVE DATE:** This ODNI Instruction becomes effective on the date of signature.



Director of the Intelligence Staff

7/25/07
Date

UNCLASSIFIED

000105

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

INSTRUCTION 80.04

Category 80 - Information and Records Management

**Office of Primary Responsibility: Intelligence Community Chief Information Officer/
Information Management Division**

Revision 1

**SUBJECT: ODNI PRE-PUBLICATION REVIEW OF INFORMATION TO BE PUBLICLY
RELEASED**

1. AUTHORITIES: The National Security Act of 1947, as amended; and other applicable provisions of law.

2. REFERENCES: Executive Order (EO) 12333, as amended; EO 13526; Controlled Access Program Coordination Office *Intelligence Community Authorized Classification and Control Markings Register and Manual (CAPCO Register)*; and the *Office of the Director of National Intelligence (ODNI) Classification Guide* dated July 3, 2012.

3. PURPOSE: This Instruction establishes the requirements and responsibilities in the ODNI for pre-publication review of all information that is to be released publicly. The goal of pre-publication review is to prevent the unauthorized disclosure of information, and to ensure the ODNI's mission and the foreign relations or security of the U.S. are not adversely affected by publication. This Instruction replaces ODNI Instruction 80.04, *Pre-publication Review of Unclassified Material for Official Dissemination*, dated August 5, 2009, and rescinds ODNI Instruction 80.14 (formerly 2007-6), *The Office of the Director of National Intelligence Instruction for ODNI Pre-publication Review of Material Prepared for Public Dissemination*, dated July 25, 2007.

4. APPLICABILITY: This Instruction applies to current and former ODNI permanent cadre employees; ODNI staff reserve (i.e., time-limited) cadre employees, including Highly Qualified Experts; federal civilian detailees; military detailees; Intergovernmental Personnel Act detailees; Presidential appointees; special government employees; assignees; and contractors (collectively, "individuals" and "personnel").

5. DEFINITIONS:

A. Chatham House Rule: An understanding, spoken or unspoken, that during academic discussions, the topics discussed and opinions relayed will NOT be attributed to individuals or organizations. This

UNCLASSIFIED

000106

UNCLASSIFIED

rule is intended to allow the free discussion of academic ideas and opinions without attribution.

B. Non-official publication: The category of publications created by ODNI personnel for personal, professional, or commercial use that will be made available to the public. (e.g., resumes, books, op-eds, personal blogs).

C. Official publication: The category of publications created by ODNI personnel as part of their duties on behalf of the ODNI, the DNI, the Intelligence Community (IC), or the U.S. Government (USG) that will be made available to the public (e.g., speeches, newsletters, official web pages, outreach documents, brochures).

D. Publication: Any information created in part (co-authored) or wholly by ODNI personnel intended for public release, regardless of the medium by which it will be released (i.e., written, voice, or electronic) that discusses operations, business practices, or information related to the ODNI, the IC, or national security.

E. Release: Allowing information to be made available to the public.

6. POLICY: The ODNI has a security obligation and legal responsibility under EO 12333 and EO 13526 to safeguard sensitive intelligence information and prevent its unauthorized publication as defined in paragraph 5.D. The Director/Information Management Division (D/IMD) or designee in the IC Chief Information Officer's (IC CIO) office will serve as the exclusive ODNI authority for approval of all ODNI public release reviews. All ODNI personnel are required to submit all official and non-official information intended for public release for review. Any 'For Official Use Only' (FOUO) information intended for State, Local, Tribal, Public Sector (SLTP) and non-Title-50 entities must be approved by the IMD. The IMD will coordinate, as necessary, with the Assistant DNI for Partner Engagement (ADNI/PE) on any FOUO information to be shared with foreign partners. FOUO information disseminated within the USG (e.g., Departments of State, Defense, Homeland Security, Treasury) does not require an IMD review. Pre-publication review must be conducted before any uncleared personnel can receive the information, and before peer review can be conducted via unsecure channels. This Instruction does not release individuals from their obligation to fully comply with nondisclosure agreements (NDAs), nor does it authorize individuals to alter the terms of such agreements. In case of any conflict between this Instruction and an NDA, the NDA shall govern. ODNI pre-publication reviews will be executed as follows:

A. Pre-submission: ODNI personnel must initiate a request for approval for the public release of information and conform to the following guidance:

(1) **Classification:** The individual initiating the request must ensure all draft documents are correctly classified and portion marked prior to submission for review. See the *CAPCO Register* and the current *ODNI Classification Guide* for guidance on correct classification and markings.

(2) **Sourcing:** Correct unclassified sourcing is critical in executing pre-publication review. ODNI personnel must not use sourcing that comes from known leaks, or unauthorized disclosures of sensitive information. The use of such information in a publication can confirm the validity of an unauthorized disclosure and cause further harm to national security. ODNI personnel are not authorized to use anonymous sourcing.

UNCLASSIFIED

(3) The Public Affairs Office (PAO) will ensure that official information intended for public release is consistent with the official ODNI position or message. The PAO will approve or disapprove the use of official ODNI seals and letterhead associated with the intended release, as deemed appropriate.

(4) Individuals must obtain supervisor approval, in accordance with internal review requirements of their component, before submitting information for pre-publication review.

(5) Contractual deliverables that will be publicly released must receive approval of the Contracting Officer (CO) or the Contracting Officer's Technical Representative (COTR) prior to submission for pre-publication review. The written approval from the CO or COTR must be included in the submission for review.

(6) ODNI personnel must, prior to participating in open discussion venues such as forums, panels, round tables, and questions and answer (Q&A) sessions, comply with the following conditions:

(a) ODNI personnel must obtain approval from the PAO to represent the ODNI in any capacity at any public forum.

(b) ODNI personnel expecting to engage in unstructured or free-form discussions about operations, business practices, or information related to the ODNI, the IC, or national security must prepare an outline of the topics to be discussed or the agenda to be followed, and provide to the IMD anticipated potential questions and ODNI responses.

(7) Required Disclaimer: Approval of non-official publications does not imply endorsement by the ODNI, IC, or national security. The following disclaimer must be provided in non-official publications created by ODNI personnel who express an opinion about the ODNI, IC, or USG:

"The views expressed in (this publication/these remarks) are the author's and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. Government agency."

This language is not required for resumes, bios, or as others exempted by the D/IMD.

B. Submission: ODNI personnel must submit requests electronically via email to **DNI-Pre-Pub**. Requests must include results from all previous pre-publication requests for the same information. Publication requests made through the Outside Activities Report (OAR) database must also include a separate email submission to **DNI-Pre-Pub WMA@cia.ic.gov** or **DNI-Pre-Pub@dni.gov** for final approval. Exceptions are as follows:

(1) Former ODNI personnel lacking access to classified email will submit requests to **DNI-Pre-Pub@dni.gov** and ensure their publications have been clearly sourced to unclassified information prior to transmittal.

(2) Detailees and assignees will submit requests for non-official publications to their home agency, provided the home agency has an established publication review process. IMD will assist those detailees and assignees uncertain of how to submit requests to their home agency.

UNCLASSIFIED

(3) The Director/Intelligence Advanced Research Projects Agency (D/IARPA) or designee is delegated the authority to review and publicly disseminate official IARPA technical publications independent of the review process outlined in this Instruction.

C. Review:

(1) The IMD will lead the coordination with all USG agencies and internal ODNI subject matter experts (SMEs) that have equities in a submitted request. The IMD will de-conflict any issues on responses from separate agencies and from within the ODNI, and will provide a single and final response to the requester.

(2) Timelines for review are determined by type of request, complexity of subject, SME time constraints, and requester deadlines. General time lines for reviews are:

(a) For Official Publications: The IMD will complete a review of official publication requests no later than 15 business days from the receipt of the request, as priorities and resources allow.

(b) For Non-Official Publications: The IMD will complete a review of non-official publication requests no later than 30 calendar days from the receipt of the request, as priorities and resources allow.

(3) Requesters must not assume approval in cases where the IMD's reply has not been received by the time guidelines described in this Instruction. It is the responsibility of the requestor to protect the information until a formal approval is provided.

D. Re-submission: In the event that a request for public release is denied in whole or in part by the IMD, the requester may resubmit the request to the IMD for a second review. The resubmittal must include results from the initial pre-publication requests, and must include additional information and/or a revised draft.

E. Appeal: If publication is denied by the IMD for a second time, the requester may submit a written appeal to the IMD no later than 30 calendar days from the date of the denial. The IMD will coordinate the appeal process. Appeal documentation must include the information intended for publication and any supporting materials to be considered. The IMD will provide the information to the Chief Management Officer (CMO) for final decision. The CMO will receive support from any USG agency and internal ODNI SMEs in the appeal decision, as appropriate. The CMO will issue a final decision, through the IMD, to the requester as time and resources allow.

F. Consequences for Non-Compliance: Failure to comply with this Instruction may result in the imposition of civil and administrative penalties, and may result in the loss of security clearances and accesses.

G. Non-attribution during discussions (Chatham House Rule): ODNI personnel who participate in environments where the Chatham House Rule applies are not authorized to discuss information or topics that are not authorized for public release.

UNCLASSIFIED

7. RESPONSIBILITIES:

A. The Chief Management Officer will:

- (1) Provide oversight for this policy and the pre-publication review process.
- (2) Issue final decisions on all formal appeals from requesters.

B. The Director/Information Management Division or designee will:

- (1) Implement this Instruction.
- (2) Serve as the final approval authority for public release of ODNI information to the public, based on classification, policy, and other applicable authorities.
- (3) Coordinate timely pre-publication reviews with all appropriate ODNI components and USG agencies. This includes obtaining, as necessary, additional information from the requester, clarification of purpose, and to make a final determination.
- (4) Provide all staff support to the CMO in the appellate process, to include the preparation of all necessary appeal information to be presented to the CMO.
- (5) Maintain records for all pre-publication review requests, dispositions, and associated actions.

C. The Director/Public Affairs Office or designee will:

- (1) Determine if ODNI personnel are authorized to officially represent the ODNI, the IC, or USG publicly.
- (2) Review official publications for accuracy, clarity, and consistency of ODNI message as part of the pre-publication review process.

D. The Director/Intelligence Advanced Research Projects Agency or designee will exercise authority granted in this Instruction to review and publicly disseminate any official IARPA technical publications independent of the review process outlined in this Instruction.

E. Component Directors will, when requested by D/IMD, designate one or more component SMEs as appropriate, either permanently or on a case-by case basis, to participate in pre-publication reviews. SMEs will limit the scope of their reviews to their component's area of expertise, and provide comments solely on the appropriateness of the information under review for public release.

8. EFFECTIVE DATE: This Instruction is effective upon signature.


Mark W. Ewing
Chief Management Officer

8 April 2014
Date



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
INSTRUCTION 80.04**

Category 80 - Information and Records Management

**Office of Primary Responsibility: Assistant Director of National
Intelligence for Policy and Strategy/
Information Management Division**

Revision 2

**SUBJECT: ODNI PRE-PUBLICATION REVIEW OF INFORMATION TO BE
PUBLICLY RELEASED**

- 1. AUTHORITIES:** The National Security Act of 1947, as amended; and other applicable provisions of law.
- 2. REFERENCES:** Executive Order (E.O.) 12333, as amended; E.O. 13526; *Intelligence Community Markings System Register and Manual*; and the *Office of the Director of National Intelligence (ODNI) Classification Guide*.
- 3. PURPOSE:** This Instruction establishes the requirements and responsibilities in the ODNI for pre-publication review of all information that is to be released publicly. The goal of pre-publication review is to prevent the unauthorized disclosure of information, and to ensure the ODNI's mission and the foreign relations or security of the U.S. are not adversely affected by publication. This Instruction replaces ODNI Instruction 80.04, *ODNI Pre-publication Review of Information to be Publicly Released*, dated April 8, 2014.
- 4. APPLICABILITY:** This Instruction applies to current and former ODNI permanent cadre employees; ODNI staff reserve (i.e., time-limited) cadre employees, including Highly Qualified Experts; federal civilian detailees; military detailees; Intergovernmental Personnel Act detailees; Presidential appointees; assignees; and contractors. In accordance with any relevant agreement by the ODNI and other government agencies (OGAs), this Instruction also applies to OGA employees providing service support to the ODNI. The above listed group will be referred to collectively as "individuals" in this Instruction.

UNCLASSIFIED

5. DEFINITIONS:

A. Chatham House Rule: An understanding, spoken or unspoken, that during academic discussions, the topics discussed and opinions relayed will NOT be attributed to individuals or organizations. This rule is intended to allow the free discussion of academic ideas and opinions without attribution.

B. Non-official publication: The category of publications created by individuals for personal, professional, or commercial use that will be made available to the public (e.g., resumes, books, op-eds, personal blogs, performance evaluation reports [PERs] for personal use).

C. Official publication: The category of publications created by individuals as part of their duties on behalf of the ODNI, the DNI, the Intelligence Community (IC), or the U.S. Government (USG) that will be made available to the public (e.g., speeches, newsletters, official web pages, outreach documents, brochures).

D. Publication: Any information created in part (co-authored) or wholly by individuals intended for release outside the control of the USG, regardless of the medium by which it will be released (i.e., written, voice, or electronic) that discusses any information related to the ODNI, the IC, or national security.

E. Release: Allowing information to be made available to the public.

6. POLICY: The ODNI has a security obligation and legal responsibility under E.O. 12333 and E.O. 13526 to safeguard sensitive intelligence information and prevent its unauthorized publication as defined in paragraph 5.D. The Director, Information Management Division (D/IMD), serves as the ODNI authority for approval of all ODNI public release reviews. All individuals are required to submit all official and non-official information intended for publication that discusses the ODNI, the IC, or national security. Any 'For Official Use Only' (FOUO) information intended for State, Local, Tribal, and Public Sector (SLTP) must be approved by the IMD. The IMD will coordinate, as necessary, with the Assistant DNI for Partner Engagement (ADNI/PE) on any FOUO information to be shared with foreign partners. FOUO information disseminated within the USG (e.g., Departments of State, Defense, Homeland Security, Treasury) does not require an IMD review. Pre-publication review must be conducted before any uncleared individuals can receive the information, and before the material is sent for peer review via unclassified channels. This Instruction does not release individuals from their obligation to fully comply with nondisclosure agreements (NDAs), nor does it authorize individuals to alter the terms of such agreements. In case of any conflict between this Instruction and an NDA, the NDA shall govern. ODNI pre-publication reviews will be executed as follows:

A. Pre-submission: Individuals must initiate a request for approval for the publication of information and conform to the following guidance:

- (1) Classification: The individual initiating the request must ensure all draft documents

UNCLASSIFIED

are correctly classified and portion marked prior to submission for review. See the *IC Markings System Register and Manual* and the current *ODNI Classification Guide* for guidance on correct classification and markings.

(2) Sourcing: Correct unclassified sourcing is critical in executing pre-publication review. Individuals must not use sourcing that comes from known leaks, or unauthorized disclosures of sensitive information. The use of such information in a publication can confirm the validity of an unauthorized disclosure and cause further harm to national security. Individuals are not authorized to use anonymous sourcing.

(3) The Public Affairs Office (PAO) will ensure that official information intended for public release is consistent with the official ODNI position or message. The PAO will approve or disapprove the use of official ODNI seals and letterhead associated with the intended release, as deemed appropriate.

(4) Individuals must obtain supervisor approval for official publication requests, in accordance with internal review requirements of their component, before submitting information for pre-publication review.

(5) Contractual deliverables that will be publicly released must receive approval of the Contracting Officer (CO) or the Contracting Officer's Technical Representative (COTR) prior to submission for pre-publication review. The written approval from the CO or COTR must be included in the submission for review.

(6) Individuals must, prior to participating in open discussion venues such as forums, panels, round tables, and questions and answer (Q&A) sessions, either in-person or online, comply with the following conditions:

(a) Individuals must obtain approval from the PAO to represent the ODNI in any capacity at any public forum.

(b) Individuals expecting to engage in unstructured or free-form discussions about operations, business practices, or information related to the ODNI, the IC, or national security must prepare an outline of the topics to be discussed or the agenda to be followed, and provide to the IMD anticipated potential questions and ODNI responses.

(7) Disclaimer: Approval of non-official publications does not imply endorsement by the ODNI, IC, or national security. Any opinions offered by individuals must be clearly marked as official ODNI or USG positions, or contain a disclaimer that the opinions are not those of the ODNI or USG. The following disclaimer is an example for a non-official publication created by an individual who expresses an opinion about the ODNI, IC, or USG:

"The views expressed in (this publication/these remarks) are the author's and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. Government agency."

UNCLASSIFIED

Disclaimers are not required for PERs, resumes, bios, or as others exempted by the D/IMD.

B. Submission: Individuals must submit requests electronically via email to DNI-Pre-Pub. Requests must include results from all previous pre-publication requests for the same information. Publication requests made through the Outside Activities Report (OAR) database must also include a separate email submission to DNI-Pre-Pub@cia.ic.gov (classified) or DNI-Pre-Pub@dni.gov (unclassified) for final approval. Exceptions are as follows:

(1) Former individuals assigned to the ODNI who, lacking access to classified email, will submit requests to DNI-Pre-Pub@dni.gov and ensure their publications have been clearly sourced to unclassified information prior to transmittal.

(2) Detailees and assignees will submit requests for non-official publications to their home agency, provided the home agency has an established publication review process. The IMD will assist those detailees and assignees uncertain of how to submit requests to their home agency.

(3) The Director, Intelligence Advanced Research Projects Agency (D/IARPA), or designee, is delegated the authority to review and publicly disseminate official IARPA technical publications independent of the review process outlined in this Instruction.

C. Review:

(1) The IMD will lead the coordination with all USG agencies and internal ODNI subject matter experts (SMEs) that have equities in a submitted request. The IMD will de-conflict any issues on responses from separate agencies and from within the ODNI, and will provide a single and final response to the requester.

(2) Timelines for review are determined by type of request, complexity of subject, SME time constraints, and requester deadlines. General time lines for reviews are:

(a) For Official Publications: The IMD will complete a review of official publication requests no later than 15 business days from the receipt of the request, as priorities and resources allow.

(b) For Non-Official Publications: The IMD will complete a review of non-official publication requests no later than 30 calendar days from the receipt of the request, as priorities and resources allow.

(3) Requesters must not assume approval in cases where the IMD's reply has not been received by the time guidelines described in this Instruction. It is the responsibility of the requester to protect the information until a formal approval is provided.

D. Re-submission: In the event that a request for public release is denied in whole or in part by the IMD, the requester may resubmit the request to the IMD for a second review. The

resubmittal must include results from the initial pre-publication requests, and must include additional information and/or a revised draft.

E. Appeal: If publication is denied by the IMD for a second time, the requester may submit a written appeal to the IMD no later than 30 calendar days from the date of the denial. The IMD will coordinate the appeal process. Appeal documentation must include the information intended for publication and any supporting materials to be considered. The IMD will provide the information to the Chief Management Officer (CMO) for final decision. The CMO will receive support from any USG agency and internal ODNI SMEs in the appeal decision, as appropriate. The CMO will issue a final decision, through the IMD, to the requester as time and resources allow.

F. Consequences for non-compliance: Failure to comply with this Instruction may result in the imposition of civil and administrative penalties, and may result in the loss of security clearances and accesses.

G. Non-attribution during discussions (Chatham House Rule): Individuals who participate in environments where the Chatham House Rule applies are not authorized to discuss information or topics that are not authorized for public release. Information that is deemed sensitive or classified due to attribution to the IC or USG cannot be discussed under the Chatham House Rule.

7. RESPONSIBILITIES:

A. The Chief Management Officer will:

- (1) Provide oversight for this policy and the pre-publication review process.
- (2) Issue final decisions on all formal appeals from requesters.

B. The Director, Information Management Division, or designee, will:

- (1) Implement this Instruction.
- (2) Serve as the approval authority for public release of ODNI information to the public, based on classification, policy, and other applicable authorities.
- (3) Coordinate timely pre-publication reviews with all appropriate ODNI components and USG agencies. This includes obtaining, as necessary, additional information from the requester, clarification of purpose, and to make a final determination.
- (4) Provide all staff support to the CMO in the appellate process, to include the preparation of all necessary appeal information to be presented to the CMO.

UNCLASSIFIED

(5) Maintain records for all pre-publication review requests, dispositions, and associated actions.

C. The Director, Public Affairs Office, or designee, will:

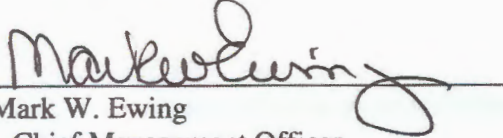
(1) Determine if individuals are authorized to officially represent the ODNI, the IC, or USG publicly.

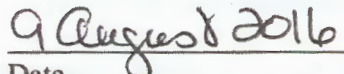
(2) Review official publications for accuracy, clarity, and consistency of ODNI message as part of the pre-publication review process.

D. The Director, Intelligence Advanced Research Projects Agency, or designee, will exercise authority granted in this Instruction to review and publicly disseminate any official IARPA technical publications independent of the review process outlined in this Instruction.

E. Component Directors will, when requested by the D/IMD, designate one or more component SMEs as appropriate, either permanently or on a case-by case basis, to participate in pre-publication reviews. SMEs will limit the scope of their reviews to their component's area of expertise, and provide comments solely on the appropriateness of the information under review for public release.

8. EFFECTIVE DATE: This Instruction is effective upon signature.


Mark W. Ewing
Chief Management Officer


Date



Prepublication Review of Information Prepared for Public Release

References:

- (a) DIA Instruction 5400.005, "Prepublication Review of Information Prepared for Public Release," 2 November 2011 (canceled)
- (b) Executive Order 12333, "United States Intelligence Activities," 4 December 1981, as amended
- (c) Executive Order 13526, "Classified National Security Information," 29 December 2009
- (d) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," 22 August 2008
- (e) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," 8 January 2009
- (f) DIA Directive 5410.400, "Public Release of Defense Intelligence Agency (DIA) Information," 16 June 2009

1. Purpose.

1.1. Replaces Reference (a).

1.2. Establishes procedures and general guidelines for the Defense Intelligence Agency's (DIA) prepublication (security and policy) review program for unclassified information and material prepared for public release.

1.3. Does not pertain to the release of information under the Freedom of Information Act, release of official information in litigation or testimony by DIA personnel as witnesses, release of information in the furtherance of an approved cover activity, or requests for declassification of classified material or "classification reviews" to determine appropriate level of classification of information.

1.4. Applies to all DIA personnel (civilian, military, and contractor), whether the information is intended to be an official or non-official product. DIA combatant command personnel releasing official command products will comply with the policies and procedures of their respective command.

2. Definitions.

2.1. Information - Any communication or representation of knowledge, such as facts, data, or opinions in any medium or form including, but not limited to, papers, articles, manuscripts, brochures, pamphlets, any video or audio media, briefings (viewgraphs and text), or other oral presentations.

2.2. Official Department of Defense (DoD) information - All information which is in the custody and control of DoD, relates to information in the custody and control of the DoD, or was acquired by DoD employees as part of their official duties or because of their official status within the DoD.

2.3. DIA information - All information which is in the custody and control of DIA, relates to information in the custody and control of DIA, or was acquired by DIA employees as part of their official duties or because of their official status within DoD or the United States (U.S.) Intelligence Community. DIA information is a sub-category of DoD information.

2.4. Official product - Material which is prepared as part of one's official duties as a DIA employee or contractor acting in an official capacity.

2.5. Non-official product - Material which is prepared by a DIA employee or contractor as a private individual and who is not acting in an official capacity for DIA, DoD, or the U.S. Government.

3. Responsibilities.

3.1. The Deputy Director will be the decision authority for appeals of review determinations when forwarded by the Director of the Office of Corporate Communications (OCC).

3.2. OCC Prepublication Review must:

3.2.1. Manage, administer, and coordinate DIA's prepublication review program.

3.2.2. Develop the DIA position regarding releasability of information submitted for review.

3.2.3. Coordinate with and obtain any necessary review by DIA directorates and special offices with relevant subject matter expertise related to or equity in the information submitted for clearance in order to develop the DIA position regarding releasability.

3.2.4. Serve as the coordination point between DIA and the DoD Office of Prepublication and Security Review (DoD OPSR) on matters relating to the DIA and DoD security and policy review programs.

DIAI 5400.005

3.2.4.1. OCC Prepublication Review will be the portal through which DoD OPSR requests DIA review of and recommendations on information proposed for public release.

3.2.4.2. As required, OCC Prepublication Review will coordinate with DoD OPSR to obtain departmental review and clearance of information submitted by DIA directorates, special offices, and personnel.

3.2.5. Serve as the coordination point of contact between DIA and the respective prepublication review components of the Intelligence Community and other agencies.

3.2.5.1. When OCC Prepublication Review reviews submissions which involve the equities of another agency, OCC Prepublication Review will coordinate its review with that agency.

3.2.5.2. OCC Prepublication Review will be the portal through which these offices request DIA review of their material intended for public release.

3.3. Directorates, special offices, and integrated intelligence centers must:

3.3.1. Submit unclassified official information and products prepared and intended for public release to OCC Prepublication Review after review and approval by component's management chain of command.

3.3.2. Conduct policy and operations security (OPSEC) reviews of their official information prior to submitting the information to OCC Prepublication Review for prepublication review. OPSEC reviews are to be accomplished by the organization's designated OPSEC program manager or program coordinator, in coordination with appropriate subject matter experts, to redact OPSEC critical information and minimize or eliminate any OPSEC indicators.

3.3.3. Provide prompt guidance and assistance when OCC Prepublication Review seeks recommendations and requests review of information proposed for public release by:

3.3.3.1. Identifying information known to be classified or warranting classification;

3.3.3.2. Identifying information which, if publicly disclosed, would jeopardize DIA, DoD, or U.S. Government interests;

3.3.3.3. Providing explanation and rationale for any objections posed to release of information;

3.3.3.4. Providing acceptable substitute language, where practical, if information conflicts with DIA or DoD policies, programs, or regulations; and

3.3.3.5. Specifying needed changes in sufficient detail to enable the author to prepare a version suitable for unclassified public release.

3.4. DIA personnel and those who are obligated by contract or non-disclosure agreements must submit information and material prepared for public release to OCC Prepublication Review for review and clearance, regardless of whether the individual is acting in an official or non-official capacity; or will obtain guidance from OCC Prepublication Review on whether information is required to be submitted.

3.5. Following separation from DIA. In accordance with Reference (d), following separation from DIA, personnel will submit for review by OCC Prepublication Review or by DoD OPSR all information or materials intended for public disclosure, including works of fiction, pertaining to intelligence, military, defense, or national security matters which may be based upon official DoD information.

4. Procedures.

4.1. Information being released in any form (written, oral, or electronic) to the public must undergo prepublication (security and policy) review if the information pertains to or mentions intelligence data; intelligence activities; military matters; national security issues; foreign relations; policies or operations of DIA, DoD, the U.S. Intelligence Community, or the U.S. Government; subjects of significant concern to DIA or DoD; or any subject about which the author has had access to classified information during his or her affiliation with DIA or DoD.

4.1.1. See Reference (e) for further delineation of information requiring review.

4.1.2. Fictional material, if it meets the criteria in paragraphs 4.1 and 4.1.1, is subject to review, as works of fiction may be based upon or can be used to convey factual information.

4.1.3. Information intended for placement on publicly accessible websites, or other publicly accessible computer servers, requires review and clearance for public release if it meets the criteria above in paragraphs 4.1., 4.1.1., or 4.1.2.

4.2. Information is submitted to OCC Prepublication Review for review through two channels: internally, from DIA directorates, special offices, and employees; or externally, from DoD OPSR or other agencies.

4.3. Submissions from DIA directorates, special offices, integrated intelligence centers, or personnel.

4.3.1. Material submitted for review should be sent to OCC Prepublication Review using the following options:

4.3.1.1. Internal electronic mail (e-mail), Joint Worldwide Intelligence Communication System (JWICS): DIA_Prepub_Rvw (this address is in the JWICS global

DIAI 5400.005

listing).

4.3.1.2. Hard copies may be submitted through internal DIA distribution.

4.3.1.3. OCC Prepublication Review will accept unclassified information proposed for public release via Non-secure Internet Protocol Router Network (NIPRNet) only after the OPSEC review and when such information is time-sensitive and the only available option. Information should be public key infrastructure (PKI) encrypted, if applicable, during transmission. The NIPRNet e-mail address is in the NIPRNet global listing as DIA_Prepub_Rvw.

4.3.2. Complete and forward the DIA Prepublication Review Request Form when submitting material for review to OCC Prepublication Review.

4.3.2.1. Official products intended for public release should be coordinated with those directorates and special offices which have equities in the material prior to submitting the product to OCC Prepublication Review. Personnel submitting official products must also obtain and indicate concurrence of their respective management chain approving the public disclosure of the product.

4.3.2.2. DIA personnel who are requesting review of material prepared in a non-official capacity must include a statement that the material submitted for review is derived from unclassified information and is, to the best of the submitter's knowledge, unclassified and appropriate for public disclosure.

4.3.3. Submissions to OCC Prepublication Review must be made prior to disclosing such information to anyone who is not authorized by DIA to have access to the material. Draft material prepared in a non-official capacity must be submitted for review at each stage of development prior to disclosing such information to anyone, such as a publisher, editor, co-author, or other member of the public, who does not have the requisite clearance and "need-to-know." This is intended to prevent comparison of different versions of the material, which could reveal items that have been deleted and determined not appropriate for public disclosure.

4.3.3.1. When personnel subject to the prepublication review requirement co-author a work, each version of the work submitted for prepublication review must clearly identify those portions of the work which were authored by the individual subject to the review requirement.

4.3.3.2. Where there is ambiguity concerning which individual wrote a section, DIA reserves the right to consider the section to be entirely written by the individual who is subject to the DIA prepublication review requirement.

4.3.4. Material submitted should be complete and include any slides, photographs, or other items to be used with the information. Notes, abstracts, or outlines will not be cleared as substitutes for a complete text. Briefings should include proposed text and remarks as well as viewgraphs and slides themselves. Abstracts to be published or presented in advance require

DIAI 5490,005

review for public release, although clearance of such an abstract will not obviate the requirement to submit the full text for clearance. Submitters are encouraged to submit completed works rather than chapters or portions of such works.

4.3.5. OCC Prepublication Review reviews the submission, obtains any necessary additional reviews by other DIA directorates or special offices, and determines DIA position regarding release.

4.3.5.1. If necessary, OCC Prepublication Review forwards the product or information to the DoD OPSR for formal departmental review, approval, and clearance, in accordance with Reference (e).

4.3.5.2. If necessary, OCC Prepublication Review forwards the product or information to other agencies whose equities are involved in the product for their review, approval, and clearance.

4.4. Review timelines. Submitters should allow OCC Prepublication Review a minimum of 10 working days for shorter items such as speeches, articles, and briefings that are non-technical in nature; 15 working days for material that is technical in nature; and 30 or more working days for lengthier or more complex items. These timelines are consistent with those of DoD and IC components and may be impacted by the extent to which material requires review by DoD OPSR or other agencies. Per DoD OPSR guidance, DIA review must be accomplished prior to obtaining DoD OPSR review and clearance.

4.5. Referrals from DoD OPSR or other agencies.

4.5.1. DoD OPSR or other agencies may refer material to DIA for review by OCC Prepublication Review. If it is determined additional review by DIA directorates or special offices is warranted, OCC Prepublication Review will task the appropriate DIA directorate or special office which has the relevant subject matter expertise to provide recommendations regarding public disclosure of information.

4.5.2. OCC Prepublication Review will develop and provide to DoD OPSR or other submitting agency the DIA position regarding release of information.

4.6. Review determinations and appeals.

4.6.1. After a full review of the material is completed, OCC Prepublication Review notifies the submitter of the results of the DIA review as follows:

4.6.1.1. Cleared for open publication. The information submitted for review may be released without restriction by the originating component. A disclaimer may be required to accompany the information. Additionally, "recommended" changes may be suggested. These changes are not binding on the author.

DIAI 5400.005

4.6.1.2. Cleared "as amended" for open publication. Amendments are binding on the submitter. Amendments may include the deletion of certain material or alternative wording of phrases and sentences.

4.6.1.3. Not cleared. The information submitted for review may not be released.

4.6.2. Although OCC Prepublication Review has no responsibility for correcting errors of fact or making editorial changes, obvious errors in the text may be identified and noted as amendments or "recommended" changes.

4.6.3. Authors who are required to amend or delete material may be required to re-submit revisions to OCC Prepublication Review for final review.

4.6.4. Appeals. Authors may request reconsideration and appeal all amendments or "not cleared" determinations. These should be in writing and offer justification or additional material to support publication.

4.6.4.1. Requests for reconsideration of determinations made by OCC Prepublication Review based on internal DIA review are to be in writing and submitted to OCC Prepublication Review.

4.6.4.2. OCC will forward the request and any additional documentation to those directorates or special offices which had objections to open publication of the product at issue.

4.6.4.3. The respective directorate's or special office's management chain will affirm or revise the determination regarding the material involving its equities, at the DISES or DISL level, and forward that recommendation to OCC Prepublication Review.

4.6.4.4. If the reconsideration is denied, the author then may appeal formally. The appeal should be in writing and, along with any supporting documentation, submitted to the Director of OCC.

4.6.4.5. The Director of OCC will consult with the Directorate and Special Office heads of the Agency components which have objections, and with other officials as appropriate.

4.6.4.6. As necessary, the Director of OCC will obtain Deputy Director decision regarding any appeal.

4.6.5. Appeals of decisions made by DoD OPSR are to be in writing and are to be addressed to the DoD OPSR, in accordance with Reference (e). Appeals may be submitted to OCC Prepublication Review for forwarding to DoD OPSR.

DIAI 5400.005

4.6.6. Appeals of decisions by other agencies are to be made in accordance with the guidance and established procedures of the respective agency.

4.7. In a non-official capacity.

4.7.1. DIA personnel may prepare information in a private and non-official capacity for disclosure in the public domain if such action:

4.7.1.1. Is not contrary to law;

4.7.1.2. Is consistent with proper ethical standards and is otherwise compatible with DIA standards of conduct;

4.7.1.3. Is not prepared during normal working hours or with the use of government facilities, property, or personnel;

4.7.1.4. Would reasonably not be expected to impair the author's performance of duties, interfere with the authorized functions of DIA or DoD, or have an adverse impact on the security or foreign relations of the U.S.;

4.7.1.5. Does not require commitments for drafts or manuscripts prior to the information being cleared; and

4.7.1.6. Does not use information unavailable to non-DoD personnel.

4.7.1.6.1. When an author asserts information intended for publication is already in the public domain, the author may be required to identify any open sources, to include official open sources, for that information and be requested to reference or cite the source of the information in a footnote.

4.7.1.6.2. Open-source information or citations may be disallowed under certain circumstances, such as when otherwise classified information appears in the public domain because of compromise or unauthorized disclosure, or when the author's DIA or DoD affiliation or position might confirm classified or OPSEC critical information.

4.7.2. DIA personnel must obtain their supervisor's concurrence prior to submission of material to OCC Prepublication Review.

4.7.2.1. Supervisory concurrence is to ensure the individual's supervisory chain has no concerns that the public disclosure would be expected to impair the performance of the individual's official duties or interfere with the authorized functions of DIA, as noted in paragraph 4.6.1.4.

4.7.2.2. Additionally, if the information pertains to the equities of the individual's office, supervisory concurrence indicates there are no objections to public disclosure

DIAI 5400.005

of the material itself.

4.8. In a DoD academic environment.

4.8.1. In the interest of academic freedom and the advancement of national defense-related concepts in the DoD school environment, students and faculty members of the National Intelligence University may prepare academic papers and manuscripts for open publication. They may express their views in such materials as long as those views do not disclose classified or OPSEC critical information or jeopardize DoD interests and the author accurately portrays official policy, even if the author takes issue with that policy.

4.8.1.1. Papers or other material prepared in response to academic requirements do not have to be submitted for review when they are not intended for release outside the academic institution.

4.8.1.2. Papers or other material is to be submitted for review and clearance if it is intended for public release or made available in libraries to which the public has access.

4.8.2. DIA personnel attending other DoD schools will submit to OCC Prepublication Review any material intended for public release or to be made available in libraries to which the public has access, unless OCC Prepublication Review defers to the review and clearance procedures of the respective DoD school being attended by DIA personnel.

4.9. In a non-DoD academic environment.

4.9.1. DIA personnel attending a non-DoD school in either an official or non-official capacity will submit for review and clearance any work or material intended for public release or which the school will make available in libraries or databases to which the public has access. Classroom work does not have to be submitted, however, if:

4.9.1.1. Classified information is not used, referenced, or divulged; and

4.9.1.2. Official information unavailable to the general public is not used.

4.9.2. DIA personnel teaching at a non-DoD school must submit their written instructional material for review and clearance if it includes classified or "for official use only" information. It is incumbent on the individual to ensure any classroom discussion or anecdotes of one's experiences in or knowledge of the Intelligence Community or the DoD do not reveal classified or otherwise sensitive information.


4.10. Use of disclaimer.

4.10.1. Approval for public release of material prepared in a non-official, private capacity or in a DoD-academic environment does not represent DIA endorsement or verification

DIAI 5400.005

of the information. Such material may be required to carry a disclaimer.

4.10.2. An appropriate disclaimer is as follows: "The views expressed in this paper [article, briefing, manuscript] are those of the author and do not reflect the official policy or position of the Defense Intelligence Agency, the Department of Defense, or the United States Government."


MICHAEL T. FLYNN
Lieutenant General, USA
Director

(U) SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE AGREEMENT

An Agreement between _____

and the United States.

(Name - Printed or Typed)

1. (U) Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or is in process of a classification determination under the standards of Executive Order 13526 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.
2. (U) I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information or material have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this agreement continue to exist whether or not I am required to sign such subsequent agreements.
3. (U) I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.
4. (U) In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation with, or show it to, anyone who is not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.
5. (U) I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 sets forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon it, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.
6. (U) I have been advised that any breach of this Agreement may result in my termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.
7. (U) I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorney's fees incurred by the United States Government may be assessed against me if I lose such action.
8. (U) I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title, or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.
9. (U) Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all conditions and obligations imposed on me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.
10. (U) Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other

Apply appropriate classification level and any control markings (if applicable) when filled in.

conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.

11. (U) I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798 and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 13526, as amended, so that I may read them at this time, if I so choose.

12. (U) I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.

13. (U) These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

14. (U) These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations rights or liabilities created by Executive Order 13526; or any successor thereto, Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosures to Congress by members of the Military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosure of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community; and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3)) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the CIA Act of 1949 (50 U.S.C. 403q(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect agent disclosure which may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Control Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

15. (U) This Agreement shall be interpreted under and in conformance with the law of the United States.

16. (U) I make this Agreement without any mental reservation or purpose of evasion.

Signature

Date

The execution of this Agreement was witnessed by the undersigned who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.

WITNESS and ACCEPTANCE:

Signature

Date

SECURITY BRIEFING / DEBRIEFING ACKNOWLEDGMENT

(Special Access Programs by Initials Only)

SSN (See Notice Below)

Printed or Typed Name

Organization

BRIEF

Date

I hereby acknowledge that I was briefed on the above SCI Special Access Program(s):

Signature of Individual Briefed

DEBRIEF

Date

Having been reminded of my continuing obligation to comply with the terms of this Agreement, I hereby acknowledge that I was debriefed on the above SCI Special Access Program(s):

Signature of Individual Briefed

I certify that the briefing presented by me on the above date was in accordance with relevant SCI procedures.

Signature of Briefing/Debriefing Officer

SSN (See notice below)

Printed or Typed Name

Organization (Name and Address)

(U) NOTICE: The Privacy Act, 5 U.S.C. 522a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397, as amended. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above, 2) determine that your access to the information has terminated, or 3) certify that you have witnessed a briefing or debriefing. Although disclosure of your SSN is not mandatory, your failure to do so may impede such certifications or determinations.